http://www.systemgroup.com

Network Servers
TriForce XP Requirements

January 7, 2005

Ensure that your server(s) and workstations meet TriForce XP Requirements.

File Server

(1) If upgrading servers, copy TriForce XP folder (F:\TRIFORCE) from old server to new server

TriForce XP must be copied on the a file Server not on a Terminal or Citrix Server. TSI Systemgroup does not support these type of installations.

(2) If upgrading servers, copy TriForce XP Downloads folder (F:\TriForce_XP_Downloads) from old server to new server

This optional step will simplify preparing new workstations.
Ensure users have read access to this folder

If it does not exist, mke a new folder **TriForce_XP_Downloads**

- Download TriForce_XP_Runtime_Setup.exe from the Systemgroup Website (Download/ Documents & Fixes/ Runtime)
- Save a shortcut to F:\TRIFORCE\CCI.EXE, rename it to **TriForce XP**

(3) Ensure users have full security access to files and subfolders of the TriForce XP folder (F:\TRIFORCE)

All users must be mapped to the same drive letter and path. Reason: if user and security settings in TriForce are related to drives/paths; mixed drive would create issues. Issues will also arise interacting with Exchange.

(4) Turn off Opportunistic Locking on the TriForce XP Windows 2000/2003 Server (see section Opportunistic Locking and Caching)

(5) Turn off caching on the hard drives where TriForce XP is stored (see section Opportunistic Locking and Caching)

Steps 4&5 must be done to avoid database corruption issues.

Terminal Server(s)

(6) Turn off Opportunistic Locking on the TriForce XP Windows 2000/2003 Server (see Opportunistic Locking and Caching)

Steps 6 must be done to avoid database corruption issues.

(7) To enable TriForce XP (same as new workstations):

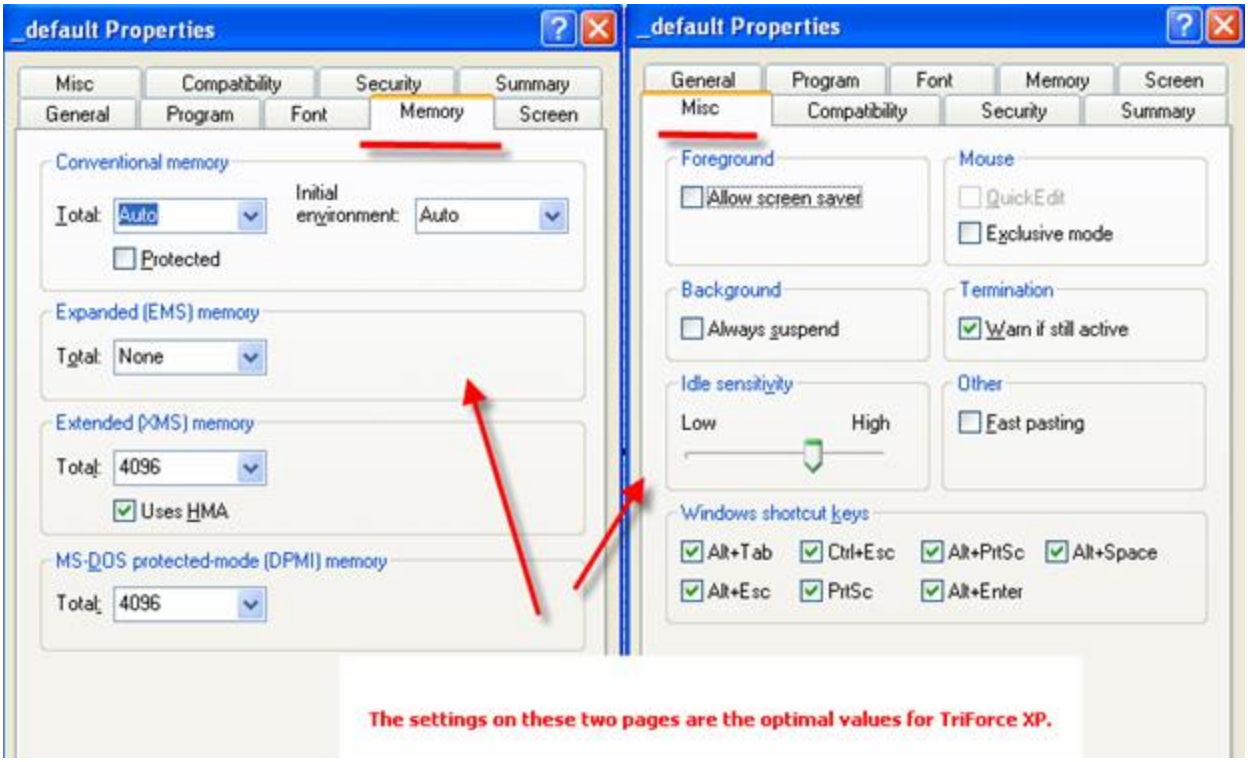
A. Install TriForce_XP_Runtime_setup.exe (execute this exe)

B. Edit C:\WINDOWS\SYSTEM32\AUTOEXEC.NT

C. Edit C:\WINDOWS\CONFIG.NT
- must have:
FILES=225
BUFFERS=40

Steps E&F required for TriForce XP administrators. When applying updates, Command windows may be executed without going through CCIVIS.PIF.

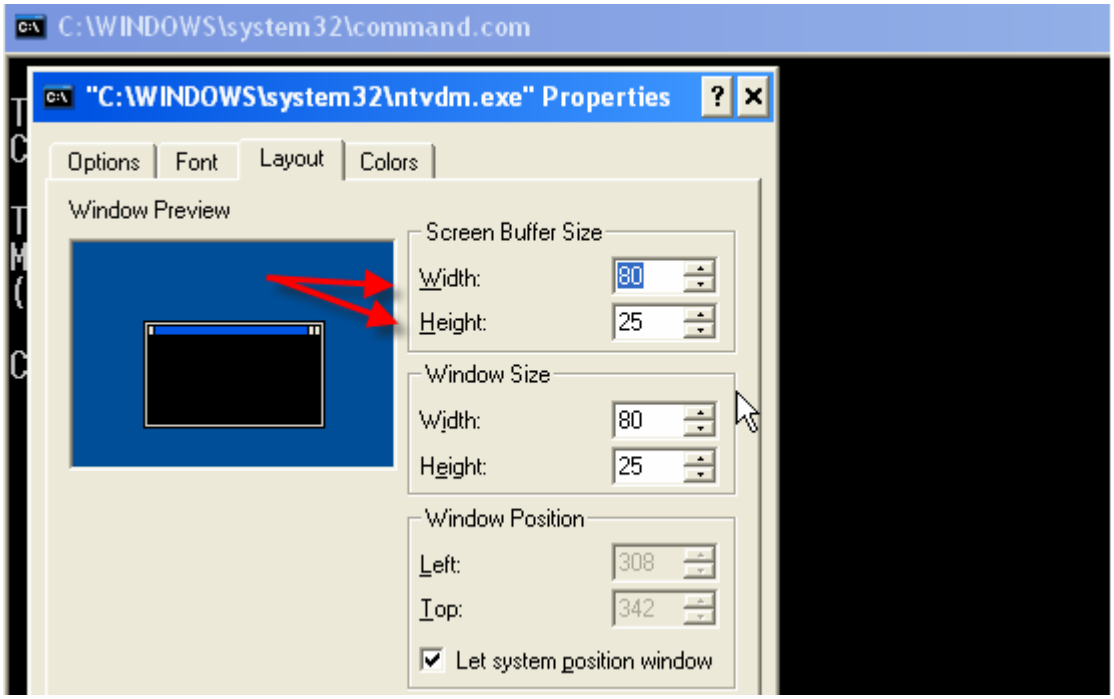
D .File **C:\WINDOWS_DEFAULT**, edit properties
Memory & Misc pages to be same like F:\TRIFORCE\CCIVIS.PIF



E. Start a Command window.

Press Start on keyboard or click Start on Windows Desktop, select run, type Command, press enter.

This will avoid error INTERNAL CONSISTENCY ERROR when applying a TriForce XP update, right-click on properties of Command window, change layout height to 25, width to 80



Workstations

(8) Turn off write caching on all workstations **(see Opportunistic Locking and Caching)**

(9) Prepare workstation for TriForce XP

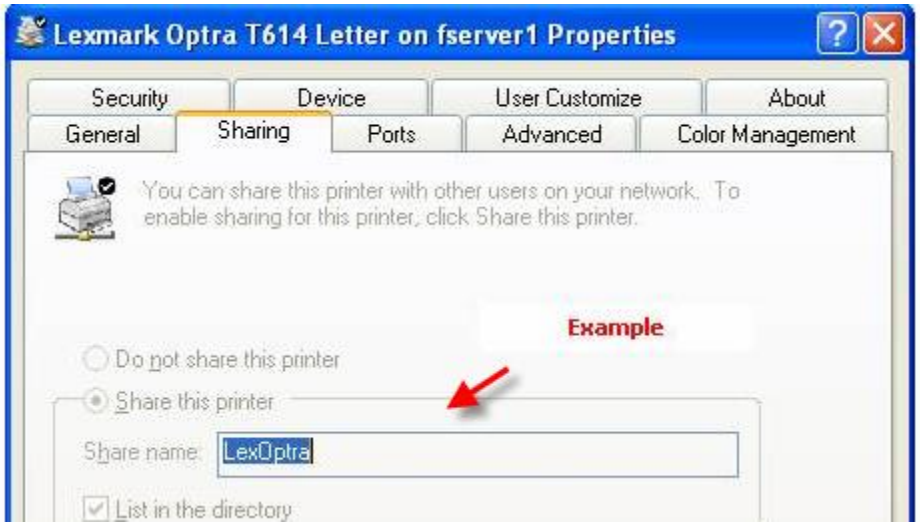
Download document **Preparing a Workstation for TriForce XP** from the Systemgroup Website (Download/ Documents & Fixes/ How To)

Summary steps:

- Check System Requirements
- Change Operating System Settings
- Install TriForce XP Runtime Setup
- Install TriForce XP Desktop Shortcut
- Install current version of Adobe Acrobat Reader

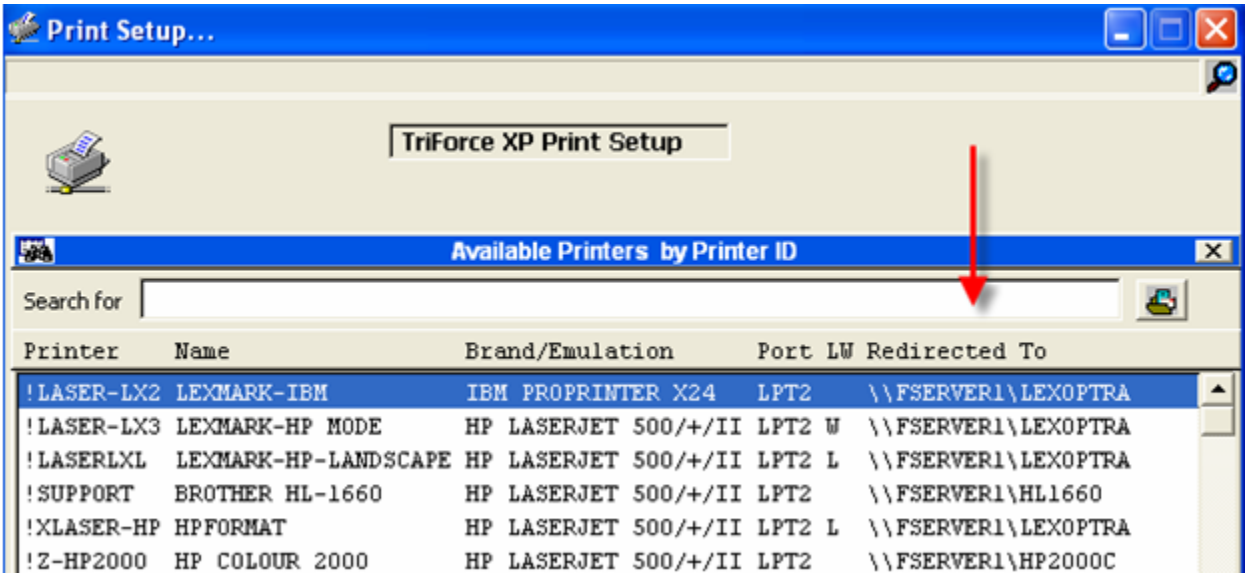
Printers and TriForce XP

(10) Printers to be used by users must be shared. Share name should be 8 characters (no spaces). This limitation is to allow support for different Windows operating systems.



(11) For TriForce Print Forms (Invoices, Sales Order, etc), printer must have PPDS support/emulation).

(12) If the server name is changed, change 'Redirected to' in FILE/ TriForce XP Print Setup…



- **Shared printers do not necessarily have to be added to each user's workstation Printers & Faxes; TriForce XP will directly print to them if you use the redirect option in the TriForce XP Printer setup.**
- **Preferably, printers attached to user workstations, should also have redirect name; if not, ensure port capturing is correctly set.**

Addendums

Opportunistic Locking and Caching

With Windows Server 2000, 2003, Microsoft has changed a standard (that used to exist in Windows NT) on how databases are updated.

- In Windows NT, caching and locking were optimized for all databases to ensure that records are properly committed to disk.
- In Windows 2000, 2003 caching and locking were optimized only for SQL Server.
  Windows Server decides when to properly commit records – irregardless of data integrity and network configurations.
- If using other databases (including Microsoft's Access, other Microsoft databases and 3rd part databases) then caching and locking must be turned off.

We researched this last year in response to issues at a company with 50+ TriForce XP users.
After our recommendations, their problems stopped.

Below is our research.

There are three main problems that may occur in busy environments:

- Duplicate system keys
- Duplicate numbers (ex: Credit Memos)
- Corrupted indexes

Summary of what has to be done on the server and workstations, based on the persistent problem:

- ensure that caching is off on the hard drives where TriForce XP is stored
- turn off Opportunistic Locking on the TriForce XP Windows 2000 Server
- ensure that write caching off on all workstations

Our research has led us to numerous instances which conclude that caching and locking must be optimized with data bases on a Windows 2000 server.

Quotes from software companies that have had these problems:

- Problems with read caching usually occur if something unforeseen happens, such as a workstation crash, where data is not properly flushed from the workstation, which can lead to data corruption
  http://www.dataaccess.com/WHITEPAPERS/OPPORTUNLOCKINGREADCACHING.HTML

- Microsoft's documentation states that "Under extreme conditions, some multi-user database applications that use a common data store over a network connection on a file server may experience transactional integrity issues or corruption of the database files and/or indexes stored on the server. This typically applies to some so-called "ISAM style", or "record oriented" multi-user database applications, not to a client/server relational system like SQL Server."
  http://www.dataaccess.com/WHITEPAPERS/OPPORTUNLOCKINGREADCACHING.HTML

- RFCB (Files Handles Caching) and Opportunistic Locking… This feature can cause problems in traditional DOS based database programs that use standard File and Record Locking (using SHARE.EXE or SHARE.386), such as our DOS Based Applications. This problem has also been reported in programs written in dBase, Clipper and Microsoft's own Access and FoxPro
  http://www.datamaster.net.au/support.html

- In practice the oplocks introduced by Microsoft are good enough when it comes to sharing files like Word documents or Excel spreadsheets in a networking environment. But they fail when it comes to heavy concurrency in environments with file-based databases such as Xbase++, Visual FoxPro and even MS-Access or VB applications with the Jet-Engine.
  http://www.superbase.com/services_tech_support_oplocks.htm

- Some settings are more important than others. Turning off NT caching (network drive caching) on the workstation and oplocks support (preferably on the server, but if you are not allowed to you may need to do it at workstation level) are probably the two most important, and in that order. None of them need be touched unless you actually experience problems such as lockouts or forms going unexpectedly inconsistent.
  http://www.dataease.co.uk/downloads/Microsoft_Registry.doc

The following pages were extracted from a web-site paper that explains the above and also includes the step-by-step procedures.

http://www.dataaccess.com/WHITEPAPERS/OPPORTUNLOCKINGREADCACHING.HTML

Opportunistic Locking and Read Caching on Microsoft Windows Networks

A Data Access Worldwide White Paper
by Dennis Piccioni

Opportunistic Locking and Read Caching on Microsoft Windows Networks

Disabling Read Caching on Windows Workstations

All Windows operating systems in the 9X family that act as database clients for Data Flex data files (meaning that they access Data Flex data files stored on other Windows PCs) need to have read caching disabled in order to minimize the chances of database corruption. This includes Windows 98 and Windows ME.

The Windows registry entry that controls read caching on Windows network clients is:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VxD\VREDIR

DiscardCacheOnOpen REG_BINARY 0 or 1
Default: 0 (not disabled)

To **disable read caching**, the value of **DiscardCacheOnOpen** must be set to **1**.

You can verify (or change or add, if necessary) this Registry value using the Windows Registry Editor (regedit.exe).
If you do change this Registry value, you will have to reboot the PC to ensure that the new setting goes into effect.

Please read the Microsoft disclaimer regarding editing of the Windows registry here.

STEPS:

1. Start > Run > **Regedit.exe**
2. Click on the + (plus sign) next to **HKey_Local_Machine**
3. Click on the + (plus sign) next to **System**
4. Click on the + (plus sign) next to **CurrentControlSet**
5. Click on the + (plus sign) next to **Services**
6. Click on the + (plus sign) next to **VxD**
7. Click on the **VREDIR** entry on the left-hand side of Registry Editor

8. If the **DiscardCacheOnOpen** registry value already exists (on the right-hand side of Registry Editor), ensure that its value is **1**

9. If the **DiscardCacheOnOpen** value already exists but its value is not **1**, double-click on **DiscardCacheOnOpen** to change its value to **1**

10. If the **DiscardCacheOnOpen** entry does not exist, right-click in the white space of the right-hand side of Registry Editor
11. Select **New** > **Binary** value
12. Rename the value to **DiscardCacheOnOpen**
13. Double-click on **DiscardCacheOnOpen** to change its value to **1**

Disabling Opportunistic Locking on Windows Servers

All Windows operating systems in the NT family that act as database servers for DataFlex data files (meaning that DataFlex data files are stored there and accessed by other Windows PCs) need to have opportunistic locking disabled in order to minimize the chances of database corruption. This includes Windows NT, Windows 2000, Windows XP and Windows 2003 Server.

There are **2** Windows registry entries that control opportunistic locking (oplocks) on Windows network servers:

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters **EnableOpLockForceClose**
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters **EnableOplocks**

1. EnableOpLockForceClose

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

EnableOpLockForceClose REG_DWORD 0 or 1
Default: 0 (not disabled)

To **disable oplocks**, the value of **EnableOpLockForceClose** must be set to **1**.

You can verify (or change or add, if necessary) this Registry value using the Windows Registry Editor (regedit.exe).
If you do change this Registry value, you will have to reboot the PC to ensure that the new setting goes into effect.

Please read the Microsoft disclaimer regarding editing of the Windows registry here.

STEPS:

1. Start > Run > **Regedit.exe**
2. Click on the + (plus sign) next to **HKey_Local_Machine**
3. Click on the + (plus sign) next to **System**

4. Click on the + (plus sign) next to **CurrentControlSet**
5. Click on the + (plus sign) next to **Services**
6. Click on the + (plus sign) next to **LanManServer**
7. Click on the **Parameters** entry on the left-hand side of Registry Editor

8. If the **EnableOpLockForceClose** registry value already exists (on the right-hand side of Registry Editor), ensure that its value is **1**

9. If the **EnableOpLockForceClose** value already exists but its value is not **1**, double-click on **EnableOpLockForceClose** to change its value to **1**

10. If the **EnableOpLockForceClose** entry does not exist, right-click in the white space of the right-hand side of Registry Editor
11. Select **New** > **DWORD** value
12. Rename the value to **EnableOpLockForceClose**
13. Double-click on **EnableOpLockForceClose** to change its value to **1**

2. EnableOplocks

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

EnableOplocks REG_DWORD 0 or 1
Default: 1 (true)

To **disable oplocks**, the value of **EnableOplocks** must be set to **0**.

You can verify (or change or add, if necessary) this Registry value using the Windows Registry Editor (regedit.exe).
If you do change this Registry value, you will have to reboot the PC to ensure that the new setting goes into effect.

Please read the Microsoft disclaimer regarding editing of the Windows registry here.

STEPS:

1. Start > Run > **Regedit.exe**
2. Click on the + (plus sign) next to **HKey_Local_Machine**
3. Click on the + (plus sign) next to **System**
4. Click on the + (plus sign) next to **CurrentControlSet**
5. Click on the + (plus sign) next to **Services**
6. Click on the + (plus sign) next to **LanManServer**
7. Click on the **Parameters** entry on the left-hand side of Registry Editor

8. If the **EnableOplocks** registry value already exists (on the right-hand side of Registry Editor), ensure that its value is **0**

9. If the **EnableOplocks** value already exists but its value is not **0**, double-click on **EnableOplocks** to change its value to **0**

10. If the **EnableOplocks** entry does not exist, right-click in the white space of the right-hand side of Registry Editor
11. Select **New** > **DWORD** value
12. Rename the value to **EnableOplocks**
13. Double-click on **EnableOplocks** to change its value to **0**

Note: The location of the registry entry for opportunistic locking has changed in Windows 2000 from the earlier location in Microsoft Windows NT. In Windows 2000, the registry entry that disables opportunistic locking is:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters

OplocksDisabled REG_DWORD 0 or 1
Default: 0 (not disabled)

To **disable oplocks**, the value of **OplocksDisabled** must be set to **1**.

Note: Windows 2000 will still respect the **EnableOplocks** registry value used to disable oplocks in earlier versions of Windows.

Disabling Opportunistic Locking on Windows Workstations

All Windows operating systems in the NT family that act as database servers for DataFlex data files (meaning that DataFlex data files are stored there and accessed by other Windows PCs) need to have opportunistic locking disabled in order to minimize the chances of database corruption. This includes Windows NT, Windows 2000 and Windows XP.

If you use a Windows NT family workstation in place of a server, you must also disable opportunistic locking (oplocks) on that workstation. For example, if you use a PC with the Windows NT **Workstation** operating system instead of Windows NT **Server**, Windows 2000 **Professional** instead of Windows 2000 **Server**, or Windows XP **Home** instead of Windows XP **Professional**, and you have DataFlex data files located on it that are accessed from other Windows PCs, you will need to disable oplocks on that system.

The major difference is the location in the Windows registry where the values for disabling oplocks are entered. Instead of the **LanManServer** location, the **LanManWorkstation** location is used here.

There are **2** Windows registry entries that control opportunistic locking (oplocks) on Windows network **workstations**:

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters **EnableOpLockForceClose**
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters **EnableOplocks**

1. EnableOpLockForceClose

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

EnableOpLockForceClose REG_DWORD 0 or 1
Default: 0 (not disabled)

To **disable oplocks**, the value of **EnableOpLockForceClose** must be set to **1**.

You can verify (or change or add, if necessary) this Registry value using the Windows Registry Editor (regedit.exe).
If you do change this Registry value, you will have to reboot the PC to ensure that the new setting goes into effect.

Please read the Microsoft disclaimer regarding editing of the Windows registry here.

STEPS:

1. Start > Run > **Regedit.exe**
2. Click on the + (plus sign) next to **HKey_Local_Machine**
3. Click on the + (plus sign) next to **System**
4. Click on the + (plus sign) next to **CurrentControlSet**
5. Click on the + (plus sign) next to **Services**

6. Click on the + (plus sign) next to **LanManWorkstation**
7. Click on the **Parameters** entry on the left-hand side of Registry Editor

8. If the **EnableOpLockForceClose** registry value already exists (on the right-hand side of Registry Editor), ensure that its value is **1**

9. If the **EnableOpLockForceClose** value already exists but its value is not **1**, double-click on **EnableOpLockForceClose** to change its value to **1**

10. If the **EnableOpLockForceClose** entry does not exist, right-click in the white space of the right-hand side of Registry Editor
11. Select **New** > **DWORD** value
12. Rename the value to **EnableOpLockForceClose**
13. Double-click on **EnableOpLockForceClose** to change its value to **1**

2. EnableOplocks

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManWorkstation\Parameters

EnableOplocks REG_DWORD 0 or 1
Default: 1 (true)

To **disable oplocks**, the value of **EnableOplocks** must be set to **0**.

You can verify (or change or add, if necessary) this Registry value using the Windows Registry Editor (regedit.exe).
If you do change this Registry value, you will have to reboot the PC to ensure that the new setting goes into effect.

Please read the Microsoft disclaimer regarding editing of the Windows registry here.

STEPS:

1. Start > Run > **Regedit.exe**
2. Click on the + (plus sign) next to **HKey_Local_Machine**
3. Click on the + (plus sign) next to **System**
4. Click on the + (plus sign) next to **CurrentControlSet**
5. Click on the + (plus sign) next to **Services**
6. Click on the + (plus sign) next to **LanManWorkstation**
7. Click on the **Parameters** entry on the left-hand side of Registry Editor

8. If the **EnableOplocks** registry value already exists (on the right-hand side of Registry Editor), ensure that its value is **0**

9. If the **EnableOplocks** value already exists but its value is not **0**, double-click on **EnableOplocks** to change its value to **0**

10. If the **EnableOplocks** entry does not exist, right-click in the white space of the right-hand side of Registry Editor
11. Select **New** > **DWORD** value
12. Rename the value to **EnableOplocks**
13. Double-click on **EnableOplocks** to change its value to **0**

Minimum System Requirements

Workstation (Desktops/Laptops)	
CPU	Pentium II 400Mhz (Minimum)
Memory	Windows ME/2000/XP: 256 MB (512 MB Preferred)
Hard Drive	IDE ATA-33 20GB
OS	Microsoft Windows ME/2000/XP (no home editions) Windows 98SE/NT** Limited support
Network Card	10/100 auto switching, preferably 3COM NIC XIRCOM PCMCIA card (for laptops).
VGA	800*600 capable
Mouse	2 buttons

Server (10 users)	
CPU	Pentium 4 (Xeon is Recommended)
Memory	1GB RAM
Hard Drive	SCSI 40MB/s Transfer
OS	Microsoft Windows 2000 Server, 2003 Server Microsoft NT 4.0 Server** Limited Support
VGA	800*600 capable Active Matrix
Mouse	2 buttons
Backup	DDS or DLT Tape drive with BackupExec or Imaging product to backup IDE discs
UPS	APC
Free HD space	4 GB or more (for TriForce XP), 20% free on partition for defragmentation utility

Server (more than 10 users)	
CPU	Dual Pentium 4 Xeon 2.8 Ghz
Memory	1GB RAM
Hard Drive	SCSI RAID 5 stripe set with parity - Ultra 160/320 (3+disks)
OS	Microsoft Windows 2000 Server, 2003 Server Microsoft NT 4.0 Server ** Limited Support
VGA	800*600 capable Active Matrix
Mouse	2 buttons
Backup	DDS or DLT Tape drive with BackupExec or Imaging product to backup IDE discs
UPS	APC
Free HD space	6 GB or more (for TriForce XP), 20% free on partition for defragmentation utility

Terminal Server	
CPU	Dual Pentium 4 Xeon 2.8 Ghz
Memory	512 MB + 60 MB per user (4GB recommended for up to 30 users)
Hard Drive	SCSI RAID 1 mirror Ultra 320 (2 disks)
OS	Microsoft Windows Terminal Server Edition 2000, 2003 (Load balancing requires 2003 Enterprise edition)
VGA	800*600 capable Active Matrix
Mouse	2 buttons
Backup	Backup or imaging agent
UPS	APC
Free HD space	18 to 36GB for system, applications and user profiles

Dot Matrix Printers	
Transaction (ex: Invoices)	Okidata 320
Check (MICR pre-printed)	Okidata 320
Label	Okidata 320

Laser Printers	
Transaction (ex: Invoices)	HP, Lexmark (with PPDS support)
Check	HP, Lexmark (with MICR code support)

Network Environment	
Desktop PC	Network Card: 3COM 10/100 3c905b, 3c905c
Laptop PC	Network Card: Xircon 10/100, 3COM, Intel
Hub	10/100 auto switching
Switch	10/100 auto switching
Wire	CAT 5

Required Software	
Office Suite	Outlook e-mail client for integrated functionality
Acrobat	Acrobat Reader (recent versions), free @ www.adobe.com

Recommended Software

Antivirus	Symantec Antivirus Corporate or Enterprise edition
Backup	Veritas BackupExec
FireWall	Microsoft ISA Server and/or hardware device (Linksys, Cisco, SonicWall)
Office Suite	Microsoft Office 2000/XP/2003

Recommended Software Updates (Service Pack / Patches)	
Windows 2000	Service Pack 4 + Security Patches
Windows XP	Service Pack 2 + most recent updates
Windows Me	With most recent updates
Office 97	Service Release 2
Office 2000	Service Pack 3
Office XP	Service Pack 2
Windows 98SE**	2nd edition
Windows NT 4.0 **	Service Pack 6a

** These products have limited support with TriForce XP 10. If issues are encountered, it is recommended that the affected workstation be upgraded to Windows XP or Windows 2000. Microsoft also has limited support as per their Product Lifecycle Policy.