Methodology in a Box™

For Citrix® Presentation Server 4.0

Running Microsoft® Windows® Server 2003

Tweaks Section

Version 4.0 Beta 4

October 22, 2006

Written by:
Douglas A. Brown

NOTICE

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. DABCC, Inc. ("DABCC"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF DABCC, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

Citrix®, MetaFrame® is a registered trademark or trademarks of Citrix Systems, Inc. in the U.S. and other countries. Windows® is a trademark of Microsoft Corporation in the U.S. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

WARNING: The information found in this document was gathered from many different sources in the Server-Based Computing world. It is provided for informational purposes only. The authors assume no responsibility for its usage. Use common sense in applying these concepts and tips. Screen shots may vary from environment to environment. Please verify correctness and applicability in a test environment first and then deploy to your production environment(s). Throughout this document, you will be required to manually edit the registry of a Terminal Server or Windows 2000 Server. Use appropriate caution before editing the registry including having a backup of your system and registry. Using Registry Editor incorrectly can cause serious system-wide problems that may require you to reinstall Windows NT or Windows 2000 to correct. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. **Use the information found in this document at your own risk.**

Please do not Sauté!

Special Thanks

As this is a document that is not developed by just one person, I wanted to take a second to thank all those who have sent me feedback on how to make it better!!

Marcel van As	Cornelio N. Framil, Jr.	Matthew Hurley
Jonathan Eyton-Williams	Mark Roles	Martin van Loenen
Paul Green	Paul Tuttle	Barry Armour
Gary Lakoskey	Rich Brumpton	Ken Puckett
Dickson Hand	Justin Doles	Jae Ellers
Darshan Arya	Evert van Maanen	Andrew Parkinson
R. Mark Robinson	Roldan Fernandez	Chris Ainger
Marco Stalder		

Special thanks to: **Jonathan Eyton-Williams** for contributing the "How to Deploy a .REG File to New and Existing Users" section.

Note: This is just the start of the thank you page. I know there are many people and web sites who have contributed to the industry tweaks doc over the years. I will be adding everyone in the next revision of this doc. If you know your name is missing then please let me know and I will make sure I add you. As I've always said, "we are nothing if we are not a group and together we will create items that are much greater than just one guy or one organization.

Table of Contents

1. How to Deploy a .REG File to New and Existing Users

Many of the registry changes referred to in this document affect the HKEY_CURRENT_USER branch of the registry. As such they need to be applied to each user session. In an initial build, these settings can be imported into default user profile to ensure that all new users start with the desired settings. If will be deploying a registry change to existing users then you will need to deploy them through a script or via a Group Policy Object.

1. 1. Initial Build/New Users

In order to do this, firstly compile the registry changes you want to make into a single file. In this file replace all instances **HKEY_CURRENT_USER** with **HKEY_USERS\defaultuser**.

For example:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Adobe\Acrobat
Reader\7.0\AVGeneral\cToolbars\cWebSearchView\cPositions\cInternal]
"bHidden"=dword:0000001

[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\Updater]
"bShowAutoUpdateConfDialog"=dword:00000000
"bShowNotifDialog"=dword:00000000
"iUpdateFrequency"=dword:00000000
```

Is changed to:

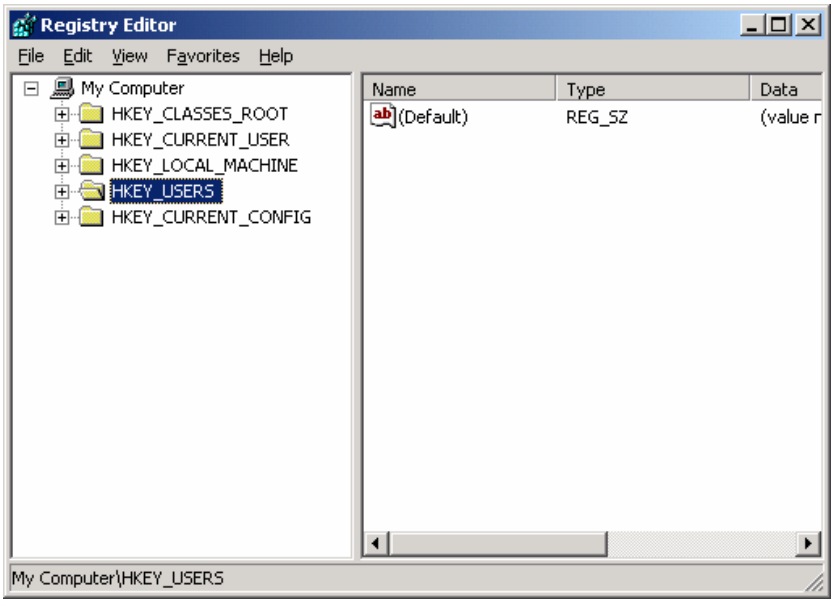
```
Windows Registry Editor Version 5.00

[HKEY_USERS\defaultuser\Software\Adobe\Acrobat
Reader\7.0\AVGeneral\cToolbars\cWebSearchView\cPositions\cInternal]
"bHidden"=dword:0000001

[HKEY_USERS\defaultuser\Software\Adobe\Acrobat Reader\7.0\Updater]

"bShowAutoUpdateConfDialog"=dword:00000000
"bShowNotifDialog"=dword:00000000
"iUpdateFrequency"=dword:00000000
```

Save this newly created file as a .reg file. Next run regedit and highlight **HKEY_USERS** as below and from the file menu bar click **File → Load Hive**.



Browse to **C:\documents and settings\default user** and select **NTUSER.DAT** (May be hidden). When prompted for a key name type **defaultuser**.

Run the customized .reg file and then don't forget to unload the default user hive by highlighting it and then go to the file menu bar and click **File → Unload Hive**

1. 2. Existing Users

Users who are already on the system and have existing profiles will need these registry changes applying to their existing profiles, as they will no longer reference the default user hive (unless their profile is recreated of course). So any additional tweaks beyond the original base build can be applied through a script in the following manner.

After you have decided upon the registry tweaks that you will be implementing then you will want to create a login script to deploy them. After the reg file is created, you can use the following sample script to deploy the registry .reg files. This script can be inserted into each server's USRLOGON.CMD to ensure that it runs for all users who log on to the server. Please note this process will apply to all users who log on to the server (including administrative users). If this is not desired consider applying a script in another way such as this using Group Policy security filtering at the OU level.

```
Rem *****Implements registry settings *****
REGEDIT -s <Path>\<Registry File Name>.REG
REGEDIT -s <Path>\<Registry File Name>.REG
REGEDIT -s <Path>\<Registry File Name>.REG
REGEDIT -s <Path>\<Registry File Name>.REG
REGEDIT -s <Path>\<Registry File Name>.REG
```

In order for this to work ensure that the Windows 2003 Group Policy setting User Configuration\Administrative Templates\System\"Prevent access to registry editing tools" is not set to disable the silent running of Regedit.

2. Tweaking Windows Server 2003 and Presentation Server 4.0

The following registry tweaks and system configurations apply to Microsoft Windows Server 2003 with Citrix MetaFrame Presentation Server 4. The goal of this section is to detail the basic tweaks needed to tune Windows for a Citrix and Terminal Services environment.

This section is broken down in to the following sections:

- Applications:
  - Adobe Acrobat
  - Internet Explorer
  - Java
  - Office 2003
  - Outlook Express
  - SAP GUI 6.40
- Disk
- Citrix MetaFrame Presentation Server
- Memory
- Microsoft Terminal Services
- Network
- Printing
- Security
- VMware
- Windows

Note: Many of the tweaks found in this document are configurable through Windows 2003 Group Policies and through Citrix Policies. Using a GPO and/or Citrix Policy could be considered a "best practice" due to the advantages of using policies for managing sets of servers instead of one server at a time. They also give you the ability to role back changes with very little effort.

When this document goes live we will also be releasing an updated "MIAB Tweaks ADM file".

The registry entries listed below have been scripted in to .REG files for your convenience. If you received this document independently from the other material (doc templates, REG file zip) then you will need to download the latest version of this doc and all the registry files discussed below from http://www.dabcc.com/miab.

IMPORTANT! This is just a draft document and we do NOT recommend you deploy these configurations in to your production environment without careful testing. Over the next few weeks we will fine tune this document to something that can be more trusted but for now, use at your own risk!

2. 1. Applications:

The following details tweaks and configurations for numerous popular applications. This is in no way a conclusive list and not all tweaks apply in all circumstances.

2. 1. 2 Adobe Acrobat 7

The following registry tweaks are specific to Adobe Acrobat 7.

Step	Description

	Remove Yahoo Search Icon from the Toolbar
	The following registry tweak removes the Yahoo Search Icon from the file menu toolbar.
	HKEY_CURRENT_USER\Software\Adobe\Acrobat
	Value Name: bHidden
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\AVGeneral\cToolbars\cWebSearchView\cPositions\cInternal]`
	`"bHidden"=dword:0000001`

	Remove the File Menu - Internet PrintMe, Update, and Purchase Options
	The following registry tweaks removes the Internet PrintMe, Update, Registration, and Purchase options from the File menu.
	HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown
	Value Name: bEFIPrintMe
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	Value Name: bPurchaseAcro
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	Value Name: bUpdater
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	Value Name: bRegisterProduct
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown]`
	`"bEFIPrintMe"=dword:00000000`
	`"bPurchaseAcro"=dword:00000000`
	`"bUpdater"=dword:00000000`
	`"bRegisterProduct"=dword:00000000`

Step	Description

	Automatically Agree to the End-User License Agreement
	
	The following registry tweak configures Adobe Acrobat to suppress the end-user requirement to agree to the EULA the first time the application starts.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\AdobeViewer
	Value Name: "EULA"
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\AdobeViewer]`
	`"EULA"=dword:00000001`

	Remove Advertisements
	
	The following registry tweak allows you to remove the advertisements in the top right hand corner of Acrobat Reader.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown
	Value Name: " bShowAdsAllow "
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown]`
	`"bShowAdsAllow"=dword:00000000`

	Disable Application Updates from Updates
	
	The following registry tweaks prevent users from being presented to install application updates.
	
	HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\Updater
	Value Name: bShowAutoUpdateConfDialog
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Value Name: bShowNotifDialog
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Value Name: iUpdateFrequency
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\7.0\Updater]`
	`"bShowAutoUpdateConfDialog"=dword:00000000`
	`"bShowNotifDialog"=dword:00000000`
	`"iUpdateFrequency"=dword:00000000`

Step	Description

	Disable Acrobat 7.0 Startup splash screen
	
	The following registry tweak allows you to disable the Adobe Acrobat 7.0 splash screen.
	
	HKEY_CURRENT_USER\ Software\Adobe\Acrobat Reader\7.0\Originals
	Value Name: bDisplayedSplash
	Data Type: DWORD
	Value Data: 0 = Disable Splash Screen, 1 = Enable Splash Screen
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\ Software\Adobe\Acrobat Reader\7.0\Originals]`
	`“bDisplayedSplash"=dword:00000000`

	Remove the “File\Create PDF Online” File Menu Item
	
	The following registry tweak allows you to remove the “File\Create PDF Online” File Menu item.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown
	Value Name: bCreatePDFOnline
	Data Type: DWORD
	Value Data: 0 = Remove the “File\Create PDF Online” item, 1 = Enable the “File\Create PDF Online Item”
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\7.0\FeatureLockdown]`
	`“bCreatePDFOnline"=dword:00000000`

2. 1. 3 Internet Explorer

The following registry tweaks are specific to Microsoft Internet Explorer 5 and above

Step	Description

	Disable Caching of (SSL) Secured Web Pages
	
	The following registry tweak controls whether SSL web pages are cached to the temporary Internet cache folder.
	
	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
	Value Name: DisableCachingOfSSLPages
	Data Type: DWORD
	Value Data: 0 = Enabled, 1 = Disabled Cache
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]`
	`“DisableCachingOfSSLPages"=dword:00000000`

	Set the Internet Explorer Window Title Text
	
	The following registry tweak sets the windows page title text.
	
	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
	Value Name: "Window Title"
	Data Type: REG_SZ
	Value Data: ”Your text here”
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]`
	`"Window Title"="Microsoft Internet Explorer provided by <Your Company Name Here>"`

	Disable Web Page Screen Flicker
	
	The following registry tweak forces off screen composition within Microsoft Internet Explorer 5 and above. This tweak will prevent against screen flicker when you view a web page that contains animated content.
	
	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
	Value Name: "Force Offscreen Composition"
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]`
	`"Force Offscreen Composition"=dword:00000001`

Step	Description
	Prevent WISP from Loading Upon Application Startup The following registry tweak allows you to prevent Acrobat's WISP service from launching upon application startup. WISP.exe started when adobe acrobat reader 7 is run. WISP is used for Abode Acrobat alternate user input. However, when you close the adobe acrobat reader 7 instance, WISP is still loaded as a process in the users environment. This can cause issues on log off and adds potentially unnecessary memory overhead for the user's session. To Remove WISP from loading apply the following reg file: Windows Registry Editor Version 5.00 [-HKEY_CLASSES_ROOT\AppID\{7F429620-16D1-471E-A81A-114992148034}] [-HKEY_CLASSES_ROOT\AppID\wisptis.EXE] [-HKEY_CLASSES_ROOT\CLSID\{04A1E553-FE36-4FDE-865E-344194E69424}] [-HKEY_CLASSES_ROOT\CLSID\{13DE4A42-8D21-4C8E-BF9C-8F69CB068FCA}] [-HKEY_CLASSES_ROOT\CLSID\{242025BB-8546-48B6-B9B0-F4406C54ACFC}] [-HKEY_CLASSES_ROOT\CLSID\{3336B8BF-45AF-429F-85CB-8C435FBF21E4}] [-HKEY_CLASSES_ROOT\CLSID\{3EE60F5C-9BAD-4CD8-8E21-AD2D001D06EB}] [-HKEY_CLASSES_ROOT\CLSID\{43B07326-AAE0-4B62-A83D-5FD768B7353C}] [-HKEY_CLASSES_ROOT\AppID\{7F429620-16D1-471E-A81A-114992148034}] [-HKEY_CLASSES_ROOT\AppID\wisptis.EXE] [-HKEY_CLASSES_ROOT\CLSID\{04A1E553-FE36-4FDE-865E-344194E69424}] [-HKEY_CLASSES_ROOT\CLSID\{13DE4A42-8D21-4C8E-BF9C-8F69CB068FCA}] [-HKEY_CLASSES_ROOT\CLSID\{242025BB-8546-48B6-B9B0-F4406C54ACFC}] [-HKEY_CLASSES_ROOT\CLSID\{3336B8BF-45AF-429F-85CB-8C435FBF21E4}] [-HKEY_CLASSES_ROOT\CLSID\{3EE60F5C-9BAD-4CD8-8E21-AD2D001D06EB}] [-HKEY_CLASSES_ROOT\CLSID\{43B07326-AAE0-4B62-A83D-5FD768B7353C}] [-HKEY_CLASSES_ROOT\CLSID\{43FB1553-AD74-4EE8-88E4-3E6DAAC915DB}] [-HKEY_CLASSES_ROOT\CLSID\{524B13ED-2E57-40B8-B801-5FA35122EB5C}] [-HKEY_CLASSES_ROOT\CLSID\{632A2D3D-86AF-411A-8654-7511B51B3D5F}] [-HKEY_CLASSES_ROOT\CLSID\{65D00646-CDE3-4A88-9163-6769F0F1A97D}] [-HKEY_CLASSES_ROOT\CLSID\{6E4FCB12-510A-4D40-9304-1DA10AE9147C}] [-HKEY_CLASSES_ROOT\CLSID\{786CDB70-1628-44A0-853C-5D340A499137}] [-HKEY_CLASSES_ROOT\CLSID\{836FA1B6-1190-4005-B434-7ED921BE2026}] [-HKEY_CLASSES_ROOT\CLSID\{8770D941-A63A-4671-A375-2855A18EBA73}] [-HKEY_CLASSES_ROOT\CLSID\{8854F6A0-4683-4AE7-9191-752FE64612C3}] [-HKEY_CLASSES_ROOT\CLSID\{937C1A34-151D-4610-9CA6-A8CC9BDB5D83}] [-HKEY_CLASSES_ROOT\CLSID\{9C1CC6E4-D7EB-4EEB-9091-15A7C8791ED9}] [-HKEY_CLASSES_ROOT\CLSID\{9DE85094-F71F-44F1-8471-15A2FA76FCF3}] [-HKEY_CLASSES_ROOT\CLSID\{9FD4E808-F6E6-4E65-98D3-AA39054C1255}] [-HKEY_CLASSES_ROOT\CLSID\{A5558507-9B96-46BA-94ED-982E684A9A6B}] [-HKEY_CLASSES_ROOT\CLSID\{A5B020FD-E04B-4E67-B65A-E7DEED25B2CF}] [-HKEY_CLASSES_ROOT\CLSID\{AAC46A37-9229-4FC0-8CCE-4497569BF4D1}] [-HKEY_CLASSES_ROOT\CLSID\{C52FF1FD-EB6C-42CF-9140-83DEFECA7E29}] [-HKEY_CLASSES_ROOT\CLSID\{D8BF32A2-05A5-44C3-B3AA-5E80AC7D2576}] [-HKEY_CLASSES_ROOT\CLSID\{DE815B00-9460-4F6E-9471-892ED2275EA5}] [-HKEY_CLASSES_ROOT\CLSID\{E3D5D93C-1663-4A78-A1A7-22375DFEBAEE}] [-HKEY_CLASSES_ROOT\CLSID\{E5CA59F5-57C4-4DD8-9BD6-1DEEEDD27AF4}] [-HKEY_CLASSES_ROOT\CLSID\{E9A6AB1B-0C9C-44AC-966E-560C2771D1E8}] [-HKEY_CLASSES_ROOT\CLSID\{EFB4A0CB-A01F-451C-B6B7-56F02F77D76F}] [-HKEY_CLASSES_ROOT\CLSID\{F0291081-E87C-4E07-97DA-A0A03761E586}] [-HKEY_CLASSES_ROOT\CLSID\{43FB1553-AD74-4EE8-88E4-3E6DAAC915DB}] [-HKEY_CLASSES_ROOT\CLSID\{524B13ED-2E57-40B8-B801-5FA35122EB5C}] [-HKEY_CLASSES_ROOT\CLSID\{632A2D3D-86AF-411A-8654-7511B51B3D5F}] [-HKEY_CLASSES_ROOT\CLSID\{65D00646-CDE3-4A88-9163-6769F0F1A97D}] [-HKEY_CLASSES_ROOT\CLSID\{6E4FCB12-510A-4D40-9304-1DA10AE9147C}] [-HKEY_CLASSES_ROOT\CLSID\{786CDB70-1628-44A0-853C-5D340A499137}] [-HKEY_CLASSES_ROOT\CLSID\{836FA1B6-1190-4005-B434-7ED921BE2026}] [-HKEY_CLASSES_ROOT\CLSID\{8770D941-A63A-4671-A375-2855A18EBA73}] [-HKEY_CLASSES_ROOT\CLSID\{8854F6A0-4683-4AE7-9191-752FE64612C3}] [-HKEY_CLASSES_ROOT\CLSID\{937C1A34-151D-4610-9CA6-A8CC9BDB5D83}]

```
[-HKEY_CLASSES_ROOT\CLSID\{9C1CC6E4-D7EB-4EEB-9091-15A7C8791ED9}]
[-HKEY_CLASSES_ROOT\CLSID\{9DE85094-F71F-44F1-8471-15A2FA76FCF3}]
[-HKEY_CLASSES_ROOT\CLSID\{9FD4E808-F6E6-4E65-98D3-AA39054C1255}]
[-HKEY_CLASSES_ROOT\CLSID\{A5558507-9B96-46BA-94ED-982E684A9A6B}]
[-HKEY_CLASSES_ROOT\CLSID\{A5B020FD-E04B-4E67-B65A-E7DEED25B2CF}]
[-HKEY_CLASSES_ROOT\CLSID\{AAC46A37-9229-4FC0-8CCE-4497569BF4D1}]
[-HKEY_CLASSES_ROOT\CLSID\{C52FF1FD-EB6C-42CF-9140-83DEFECA7E29}]
[-HKEY_CLASSES_ROOT\CLSID\{D8BF32A2-05A5-44C3-B3AA-5E80AC7D2576}]
[-HKEY_CLASSES_ROOT\CLSID\{DE815B00-9460-4F6E-9471-892ED2275EA5}]
[-HKEY_CLASSES_ROOT\CLSID\{E3D5D93C-1663-4A78-A1A7-22375DFEBAEE}]
[-HKEY_CLASSES_ROOT\CLSID\{E5CA59F5-57C4-4DD8-9BD6-1DEEEDD27AF4}]
[-HKEY_CLASSES_ROOT\CLSID\{E9A6AB1B-0C9C-44AC-966E-560C2771D1E8}]
[-HKEY_CLASSES_ROOT\CLSID\{EFB4A0CB-A01F-451C-B6B7-56F02F77D76F}]
[-HKEY_CLASSES_ROOT\CLSID\{F0291081-E87C-4E07-97DA-A0A03761E586}]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\1125549C421D34E4DBF1036F62580BE1]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\652A08B235C6DFF4C8CD41B52DE68CA4]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\9B4B5940D4625D64C85532B8CDE3BF4D]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\D656DA4A9E277A34D90D5E6FFA34E827]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\7040110900063D11C8EF10054038389C\Features\WISPFiles]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\7040110900063D11C8EF10054038389C\Features\WISPHidden]
[-HKEY_CLASSES_ROOT\TpcCom]
[-HKEY_CLASSES_ROOT\TpcCom.ClassicW]
[-HKEY_CLASSES_ROOT\TpcCom.ClassicW.1]
[-HKEY_CLASSES_ROOT\TpcCom.DrawAttrs]
[-HKEY_CLASSES_ROOT\TpcCom.DrawAttrs.1]
[-HKEY_CLASSES_ROOT\TpcCom.DrawAttrsXP]
[-HKEY_CLASSES_ROOT\TpcCom.DrawAttrsXP.1]
[-HKEY_CLASSES_ROOT\TpcCom.GenericRecognizer]
[-HKEY_CLASSES_ROOT\TpcCom.GenericRecognizer.1]
[-HKEY_CLASSES_ROOT\TpcCom.InkObject]
[-HKEY_CLASSES_ROOT\TpcCom.InkObject.1]
[-HKEY_CLASSES_ROOT\TpcCom.InkObjectXP]
[-HKEY_CLASSES_ROOT\TpcCom.InkObjectXP.1]
[-HKEY_CLASSES_ROOT\TpcCom.InkSettings.1]
[-HKEY_CLASSES_ROOT\TpcCom.Lattice.1]
[-HKEY_CLASSES_ROOT\TpcCom.RecoManager]
[-HKEY_CLASSES_ROOT\TpcCom.RecoManager.1]
[-HKEY_CLASSES_ROOT\TpcCom.TabletManager]
[-HKEY_CLASSES_ROOT\TpcCom.TabletManager.1]
[-HKEY_CLASSES_ROOT\TpcCom.UserDictionary]
[-HKEY_CLASSES_ROOT\TpcCom.UserDictionary.1]
[-HKEY_CLASSES_ROOT\TypeLib\{194508A0-B8D1-473E-A9B6-851AAF726A6D}]
[-HKEY_CLASSES_ROOT\TypeLib\{56D04F5D-964F-4DBF-8D23-B97989E53418}]
[-HKEY_CLASSES_ROOT\TypeLib\{773F1B9A-35B9-4E95-83A0-A210F2DE3B37}]
[-HKEY_CLASSES_ROOT\TypeLib\{7D868ACD-1A5D-4A47-A247-F39741353012}]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\1125549C421D34E4DBF1036F62580BE1]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\652A08B235C6DFF4C8CD41B52DE68CA4]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\9B4B5940D4625D64C85532B8CDE3BF4D]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\D656DA4A9E277A34D90D5E6FFA34E827]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\7040110900063D11C8EF10054038389C\Features\WISPFiles]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\7040110900063D11C8EF10054038389C\Features\WISPHidden]
```

2. 1. 4 Java

The following registry tweaks are specific to Sun Java JRE

Step	Description

	Turn off Java Automatically Update
	
	The following registry tweak turns off the automatic update feature in the Sun Java Runtime Environment.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy
	Value Name: "EnableJavaUpdate"
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy]`
	`"EnableJavaUpdate"=dword:00000000`

	Disable Java Automatic Updates Application from Running upon Login
	
	The following registry tweak removes the SunJavaUpdateSched program from running when a user logs on to the Terminal Server.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
	Value Name: "SunJavaUpdateSched "
	Data Type: : REG_SZ
	Value Data: Delete the key
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]`
	`"SunJavaUpdateSched"=-`

	Hide Java System Tray Icon
	
	The following registry tweak hides the Java System Tray Icon.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Plug-in\1.5.0_06
	Value Name: "HideSystemTrayIcon"
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Plug-in\1.5.0_06]`
	`"HideSystemTrayIcon"=dword:00000001`
	
	Note: The above registry setting is dependant upon the version of Java have installed on the server. In the above case it is version 1.5.0_06.

2. 1. 5 Office 2003

The following registry tweaks are specific to Microsoft Office 2003

Step	Description

	Disable 'Customer Experience Improvement Program' in Office 2003
	
	The following registry tweak disables Microsoft Office 2003 from being prompted to participate in the Customer Experience Improvement Program.
	
	HKEY_CURRENT_USER\Software\Microsoft\Office\Common
	Value Name: QMEnable
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Office\Common]`
	`"QMEnable"=dword:00000000`

	Turn off Speech and Handwriting Recognition Features
	
	The following registry tweak disables the Office Speed and Handwriting recognition features. These features are launched through the Ctfmon.exe file. By default, the Office features and components that require the Ctfmon.exe file are turned off during installation in a Terminal Server environment. Although these features can be enabled through a custom installation, Microsoft recommends that CTFMON remain disabled in a Terminal Server environment because of potential performance issues.
	
	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
	Value Name: ctfmon.exe
	Value Type: DWORD
	Value Data: delete the key
	
	HKEY_CURRENT_USER\Software\Microsoft\CTF
	Value Name: Disable Thread Input Manager
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	HKEY_CURRENT_USER\Software\Microsoft\CTF\MSUTB
	Value Name: ShowDeskBand
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]`
	`"ctfmon.exe"=-`
	
	`[HKEY_CURRENT_USER\Software\Microsoft\CTF]`
	`"Disable Thread Input Manager"=dword:00000001`
	
	`[HKEY_CURRENT_USER\Software\Microsoft\CTF\MSUTB]`
	`"ShowDeskBand"=dword:00000000`
	
	For more information please visit Microsoft support article: How to turn off the speech recognition and the handwriting recognition features in Office 2003

Step	Description

	Disable Outlook 2003 'Welcome to Outlook' Message
	
	The following registry tweak disables Outlook 2003 from creating a "Welcome to Outlook" message the first time a user logs in.
	
	HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Setup
	Value Name: CreateWelcome
	Value Type: DWORD
	Value Data: FFFFFFFF
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Setup]`
	`"CreateWelcome"=dword:FFFFFFFF`

2. 1. 6 SAP GUI 6.40

The following registry tweaks are specific to SAP GUI version 6.40.

Step	Description

	Configure the SAPWorkdir
	
	The following registry tweak allows you to configure the SAPWorkdir. The SAPWorkdir is the SAP GUI for Windows Temp Directory. All temp files and history files are stored within the SAPWorkdir. It is not possible to separate the content of the SAPWorkdir. For example, you cannot save the SAP GUI for Windows History at one location and the Temp files at another.
	
	It is recommended to centralize the SAPWorkdir for each user. It should be located on the user's home drive on a centralized fileshare. This prevents uploading and downloading during logon and logoff. Also, having only one SAPWorkdir per user is a great benefit in a Citrix farm with more than one server.
	
	HKEY_LOCAL_MACHINE\\Software\SAP\SAP Shared
	Value Name: SAPworkdir
	Value Type: REG_EXPAND_SZ
	Value Data: This key has to be user-independent (For example, %userhome%\sapworkdir or h:\sapworkdir dependent on your infrastructure) to ensure multi-user compatibility. SAP stores temporary files and the history in this folder.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\\Software\SAP\SAP Shared]`
	`"SAPworkdir"=”%userhome%\sapworkdir”`

	Disable SAP Auto Updates The following registry tweak allows you to disable SAP GUI auto updates. By default, SAP GUI will try to connect to the update server each time it is started. And if updates are available, they will be automatically installed on the environment. If the user has no administrative rights this could have impacts on the performance. To disable SAP auto updates you will need to delete the following registry key: HKEY_LOCAL_MACHINE\Software\SAP\SAPSetup\SAPstart\AutoUpdate

	Disable the SAP GUI for Windows Splash Screen
	
	The following registry tweak disables the SAP GUI for Windows splash screen.
	
	HKEY_LOCAL_MACHINE\Software\SAP\General\Appearance
	Value Name: SplashOff
	Value Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\SAP\General\Appearance]`
	`"SplashOff"=dword:00000000`

Step	Description

	Disable SAP GUI Animation
	
	The following registry tweak disables the waiting time animation in Enjoy mode.
	
	HKEY_LOCAL_MACHINE\Software\SAP\General\Appearance
	Value Name: Animation
	Value Type: REG_SZ
	Value Data: "Off"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\SAP\General\Appearance]`
	`"Animation"="”Off”`
	
	Close SAPLogon when the last SAP connection is closed.
	
	The following registry tweak allows you to close the SAPLogon when once the last SAP connection is closed.
	
	HKEY_LOCAL_MACHINE\Software\SAP\SAPLogon
	Value Name: Autoclose
	Value Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\SAP\SAPLogon]`
	`"Autoclose"=dword:00000001`
	
	Optimizing SAP for Citrix Password Manager
	
	The following registry tweak will allow you to configure SAP to display the proper Windows title bar name.
	
	As of Patch 2 for SAP GUI 6.40 for Windows, you can display the additional windows title by setting the "ShowAdditionalTitleInFo" registry key. This is necessary to allow Citrix Password Manager to distinguish between different SAP back ends.
	
	HKEY_LOCAL_MACHINE\Software\SAP\SAPGUI Front\SAP Frontend Server\\Administration
	Value Name: ShowAdditionalTitleInFo
	Value Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\SAP\SAPGUI Front\SAP Frontend Server\\Administration]`
	`"ShowAdditionalTitleInFo"==dword:00000001`

Note: For more information on implementing SAP GUI 6.40 on a Citrix Presentation Server please refer to the following Citrix white paper:

http://support.citrix.com/servlet/KbServlet/download/9620-102-14774/SAP%20GUI%206_40%20for%20Windows%20WP.pdf

2. 2. Disk Subsystem

The following details tweaks and configurations for the Windows Disk Subsystem. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Disabling File Locking
	
	The following registry tweak specifies whether the 'lock-and-read' and 'write-and-unlock' performance enhancements are enabled. These features improve performance when an application locks data and then immediately reads the data, or writes data and then immediately unlocks it. It is known that this causes problems with some database applications, with their own locking mechanisms. For example, MS Access and/or JET database.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
	Value Name: UseLockReadUnlock
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]`
	`"UseLockReadUnlock"=dword:00000001`

	Tuning the File System - Preventing File Access Stamp Updates
	
	The following registry tweak specifies whether NTFS updates the last-accessed timestamp of a file when that file is opened. Because updating the last-accessed timestamp requires writing data to the disk it might be faster if this type of update is disabled. However, some applications may require that files have an accurate last-accessed timestamp.
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
	Value Name: NtfsDisableLastAccessUpdate
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]`
	`"NtfsDisableLastAccessUpdate"=dword:00000001`

Step	Description

	Disable Lazy Writes
	
	The following registry tweaks allows you to disable lazy writes. Lazy writes occur when data is cached instead of immediately written to disk, which is the default. If data is being sent across the network or the server has a caching controller card, disabling lazy writes improves performance.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
	Data Type: DWORD
	Value Name: IRPStackSize
	Value: 15
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\LanmanWorkStation\Parameters
	Data Type: DWORD
	Value Name: UtilizeNTCaching
	Value: 0
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]`
	`"IRPStackSize"=dword:0000000f`
	
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\LanmanWorkStation\Parameters]`
	`"UtilizeNTCaching"=dword:00000000`

2. 3. Citrix MetaFrame Presentation Server - ICA

The following details tweaks and configurations for Citrix MetaFrame Presentation Server. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Disable Citrix Client Audio Mapping
	The following registry tweak will disable Citrix Client Audio Mapping.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp
	Value Name: fDisableCam
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp]`
	`"fDisableCam"=dword:00000001`

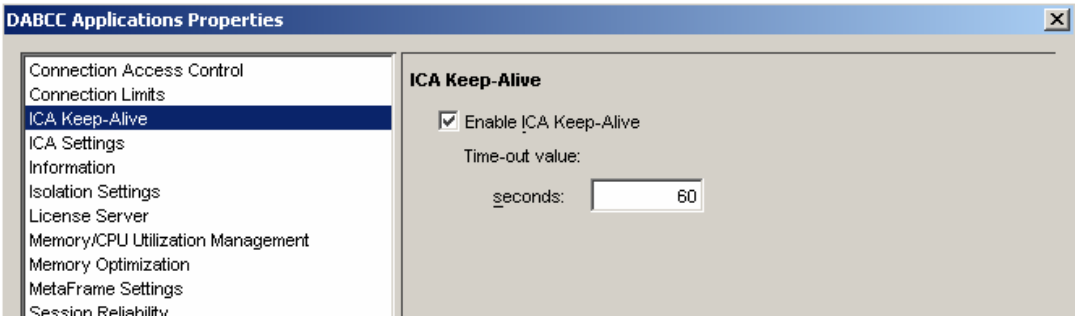
	Disable Citrix Client COM Port Mapping
	The following registry tweak allows you to disable the Citrix Client COM Port Mapping virtual channel.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp
	Value Name: fDisableCcm
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp]`
	`"fDisableCcm"=dword:00000001`

	Set User Interface and Environment Related Items, Per User
	The following registry tweak allows you to configure the user interface and environment settings on a per user basis. This includes configurations for such items as, wallpaper, animation effects, and screen savers.
	
	HKEY_CURRENT_USER\Control Panel\Desktop
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Control Panel\Desktop]`
	`"CursorBlinkRate"="1200"`
	`"DragFullWindows"="0"`
	`"WaitToKillAppTimeout"="20000"`
	`"AutoEndTasks"="1"`
	`"MenuShowDelay"="10"`
	`"SmoothScroll"=dword:00000000`

Step	Description

	Optimize the User Interface for a Citrix ICA Connection
	
	The following registry tweak allows you to configure the user interface and environment settings on a per Citrix Server basis. This includes configurations for such items as, wallpaper, animation effects, and screen savers.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp\UserOverride\Control Panel\Desktop
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp\UserOverride\Control Panel\Desktop\WindowMetrics
	
	Note: - This tweak only affects users who have **not** already created their Citrix Server profile.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp\UserOverride\Control Panel\Desktop]`
	`"AutoEndTasks"="1"`
	`"MenuShowDelay"="10"`
	`"CursorBlinkRate"="-1"`
	`"DragFullWindows"="0"`
	`"WaitToKillAppTimeout" = "20000"`
	`"SmoothScroll" = dword:00000000`
	`"Wallpaper" = "(none)"`
	
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ICA-tcp\UserOverride\Control Panel\Desktop\WindowMetrics]`
	`“MinAnimate"="0"`

	Killing Processes On logoff
	
	The following registry tweak addresses processes that do not close down properly when a uses logs out of a seamless application:
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
	Value Name: DllName
	Data Type:
	Value Data: “seamls20.dll"
	
	Value Name: NotifyEvent
	Data Type:
	Value Data: “WfshellTwiNotify"
	
	Value Name: LogoffCheckSysModules
	Data Type:
	Value Data: “ssoshell.exe,ssobho.exe,ssomho.exe,acrodist.exe,acrotray.exe"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI]`
	`"DllName"="seamls20.dll"`
	`"NotifyEvent"="WfshellTwiNotify"`
	`"LogoffCheckSysModules"="ssoshell.exe,ssobho.exe,ssomho.exe,acrodist.exe,acrotray.exe"`

Step	Description
	Enable ICA Keep-Alives on Citrix MetaFrame Presentation Servers The following tweak allows you to enabled ICA Keep-Alives. When users are disconnected from an ICA session due to a physical or other network issue their connection may still appear as active. If they then try to reconnect they will not be able to reconnect to their existing session and will be logged into a new session. When ICA Keep-Alives are enabled the Citrix server will send packets to the client to determine if the connection is still open. If the client device does not respond then the session is placed in to disconnect mode. To enable ICA Keep-Alives you will need to right click the Farm node in the Citrix Presentation Server Management Console and click **Properties** → click the **ICA Keep-Alive** node and then click to enable the **Enable ICA Keep-Alive** checkbox. The **Time-out value** text box allows you to specify the interval in which the ICA Keep-Alive packages are sent to the client. If the client device does not respond within the **Time-out value** the session is set to disconnected mode. The time-out value can be set between 1 and 3600 seconds.  **Important**: When launching a published application with Session Reliability, ICA KeepAlive **does not function**. With Session Reliability, after an ICA session is disconnected on the client side, the session might be recognized as in "active" status longer than the **Sessions to keep active** setting indicates.
	Enable ICA Keep-Alives on Servers Running Secure Gateway for MetaFrame If you will be implementing Citrix Secure Gateway for MetaFrame servers then you will be required to enabled ICA keep-Alives on the servers in order to gain the benefits of the of ICA Keep-Alives, as stated above. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix Value Name: IcaEnableKeepAlive Value Type: DWORD Value Data: 0 = Disabled, 1 = Enabled Value Name: IcaKeepAliveInterval Value Type: DWORD Value Data: 1 – 3600 (decimal) ***Recommended .reg file text:*** Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix] "IcaEnableKeepAlive"=dword:00000001 "IcaKeepAliveInterval"=dword:0000003c

Step	Description

	Configure Program Neighborhood Agent URL
	
	The following registry tweak will allow you to configure the Citrix Program Neighborhood Agent to point to a predefined URL.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Program Neighborhood Agent
	Value Name: Config URL
	Value Type: REG_SZ
	Value Data: <url of the Web Interface Server running the Program Neighborhood Agent Portal>
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Program Neighborhood Agent]`
	`“Config URL"=”http://webserver.local/Citrix/PNAgent/config.xml`

2. 4. Memory Tweaks

The following details tweaks and configurations for the Windows Memory subsystem. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Improving Windows Kernel Performance
	
	The following registry tweak specifies whether kernel-mode drivers and kernel-mode system code can be paged to disk when not in use. Even if you have enough RAM available, Windows will still "page" important operating system components to the pagefile. By enabling the DisablePagingExecutive registry key you will prevent Windows from paging this type of data.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
	Value Name: DisablePagingExecutive
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]`
	`"DisablePagingExecutive"=dword:00000001`

	Clear Page File on System Shutdown
	
	The following registry tweak specifies whether inactive pages in the paging file are filled with zeros when the system stops. This is a Windows Server 2003 security feature that prevents the pages from being read by another process.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
	Value Name: ClearPageFileAtShutdown
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]`
	`"ClearPageFileAtShutdown"=dword:00000001`
	
	Note: Implementing this tweak could cause an increase in the time it takes to shutdown the server. If you are in a secure environment I recommend this tweak, if not then beware it will take more time to shutdown the server.

Step	Description

	Increase the Network Request Buffer
	
	The following registry tweak can allow you to gain additional performance by modifying the network request buffer size on the Terminal Server. The SizReqBuf value determines how much data is buffered at one time to send to a client. Increasing this value to 65,536 bytes from the default of 4,356 bytes significantly improves LAN Manager file writes.
	
	The minimum setting is 1024. Small buffers use less memory, and large buffers can improve performance. The exact value that works best in a particular environment depends on the specific configuration of that environment. For an optional value, try 4410 (hexadecimal); this has been shown to work well in a fairly standard Ethernet environment. By default, this setting is 4356 bytes on computers. On servers that have more than 512 MB of memory, this value is increased to 16 KB. A receive buffer that is larger can improve performance on query directory and similar commands, but at the price of more memory per work item.
	
	Increasing the SizReqBuf value can increase performance significantly in a high-latency environment. However, note that increasing the SizReqBuf value also increases the non-paged pool memory that is used by the LanManServer service. If you increase the SizReqBuf value, monitor non-paged pool to make sure that the change does not affect the performance of the file server. Increasing the SizReqBuf value also proportionately increases the risk that a malicious user might exhaust non-paged pool on the file server.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
	Value Name: SizReqBuf
	Data Type: DWORD
	Value Data: 512 – 65535
	
	For more information please visit: http://support.microsoft.com/?kbid=320829
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]`
	`"SizReqBuf"=dword:00003904`

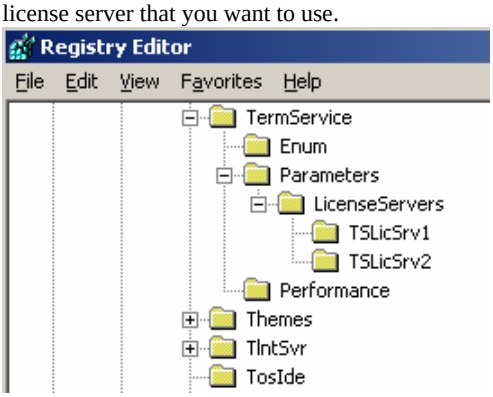
2. 5. Microsoft Windows Terminal Server - RDP

The following details tweaks and configurations for Microsoft Terminal Services RDP connections. This is in no way a conclusive list and not all tweaks apply in all circumstances.

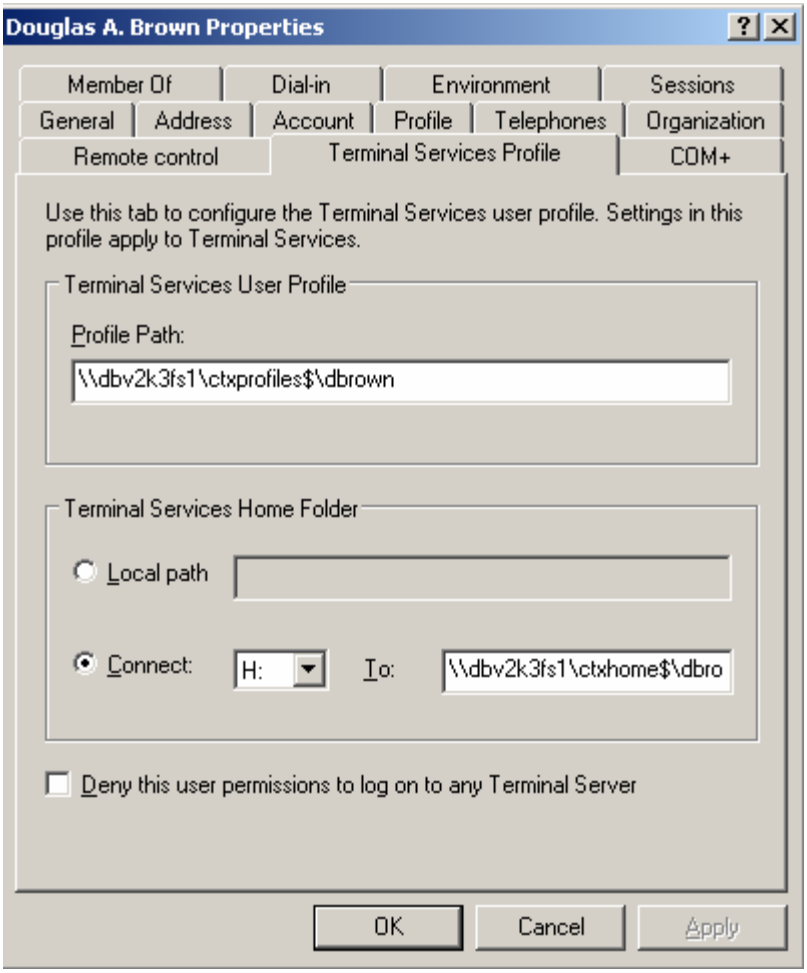
Step	Description

	Optimize the User Interface for a Terminal Server RDP Connection
	
	The following registry tweak allows you configure user interface and environment settings on a per Terminal Server only basis. Configurations for such items as, wallpaper, animation effects, and screen savers. This tweak only affects users who have not already created their Terminal Server profile.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp\UserOverride\Control Panel\Desktop
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp\UserOverride\Control Panel\Desktop\WindowMetrics
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp\UserOverride\Control Panel\Desktop]`
	`"AutoEndTasks"="1"`
	`"MenuShowDelay"="10"`
	`"CursorBlinkRate"="1200"`
	`"DragFullWindows"="0"`
	`"WaitToKillAppTimeout" = "20000"`
	`"SmoothScroll" = dword:00000000`
	`"Wallpaper" = "(none)"`
	
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp\UserOverride\Control Panel\Desktop\WindowMetrics]`
	`“MinAnimate"="0"`

	Change the Listening Port for an RDP Connection
	
	The following tweak allows you to change the port used by the RDP protocol.
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber
	Value Name: PortNumber
	Value Type: DWORD
	Value Data: 1-5000 (decimal)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber]`
	`"PortNumber" = dword: 00000D3D`

Step	Description
	Hardcode a Preferred Terminal Services License Server The following registry tweak allows you to hardcode the preferred Terminal Services License Server. 1. Browse to the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters** 2. Click **Edit** from the File Menu bar → click **New** → click **Key** → enter "**LicenseServers**" as the name of the new key. 3. Click the newly created **LicenseServers** key and click **Edit** from the File Menu bar → click **New** → click **Key** → enter the NetBIOS name, or the fully qualified domain name (FQDN), or the IP Address of the license server that you want to use.  4. Repeat step 3 for any additional license servers. For more information please refer to: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B279561

Step	Description
	Configure the User Terminal Server Profile, Drive, and Home Folder Path The following Visual Basic Script allows you to configure the Terminal Services Profile configuration settings, including the Terminal Services User Profile, Terminal Services Home Folder, and Drive Letter to on all users in an Windows Server 2003 Active Directory domain.




```
Const Enabled = 1
Const Disabled = 0
Set objUser = GetObject("LDAP://cn=user,ou=test,dc=citrix,dc=com")

objUser.TerminalServicesProfilePath = ""
objUser.TerminalServicesHomeDirectory = ""
objUser.TerminalServicesHomeDrive = ""
objUser.AllowLogon = Enabled

objUser.SetInfo
```

2. 6. Network Tweaks

The following details tweaks and configurations for the Windows Network subsystem. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Set Mapped Network Drives as Non-Persistent by default
	
	The following registry tweak specifies if a network drive will be recreated each time the user logs on. By default, network drives within Windows are persistent. This tweak allows you to make the default of all newly created network drivers as non-persistent, thus the next time the user logs on the network drives are not connected.
	
	HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections
	Value Name: SaveConnections
	Value Type: REG_SZ
	Value Data: "no"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections]`
	`"SaveConnections"="no"`

	Disable Retaining Recently Accessed Shares in My Network Places
	
	The following registry tweak specifies whether Windows will retain recently accessed shares to the My Network Places folder.
	
	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
	Value Name: NoRecentDocsNetHood
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]`
	`"NoRecentDocsNetHood"=dword:00000001`

Step	Description

	Improving Connectivity over Inconsistent WAN Links
	
	The following registry tweak allows you to improve connectivity over inconstant WAN links and prevent sessions from being disconnected for no real reason. If the quality of a WAN link dramatically decreases after a user connects to a Terminal Server, i.e. your using a Cable modem and additional users logon, the connection can be dropped.
	
	The TcpMaxDataRetransmissions entry specifies how many times TCP retransmits an unacknowledged data segment on an existing connection. TCP retransmits data segments until they are acknowledged or until this value expires, at which time the connection is dropped.
	
	TCP/IP adjusts the frequency of retransmissions over time. TCP establishes an initial retransmission interval by measuring the round trip time on the connection. The interval doubles with each successive retransmission on a connection, and it is reset to the initial value when responses resume.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
	Value Name: TcpMaxDataRetransmissions
	Data Type: DWORD
	Value Data: 10 (decimal)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]`
	`"TcpMaxDataRetransmissions"=dword:0000000a`

	Enable TCP Keep-Alives
	
	The following registry tweak allows you to configure TCP KeepAlives. They work just like ICA Keep-Alives do and are required to be implemented along side ICA Keep-Alives on both Citrix servers and Secure Gateway server.
	
	KeepAliveTime specifies how often TCP sends keep-alive transmissions. TCP sends keep-alive transmissions to verify that an idle connection is still active.
	
	KeepAliveInterval Specifies how often TCP repeats keep-alive transmissions when no response is received. TCP sends keep-alive transmissions to verify that idle connections are still active. This prevents TCP from inadvertently disconnecting active lines.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
	Value Name: KeepAliveTime
	Data Type: DWORD
	Value Data: 1–16777215 (decimal in milliseconds and 1,000 milliseconds = 1 second)
	
	Value Name: KeepAliveInterval
	Value Type: DWORD
	Value Data: 1–16777215 (decimal in milliseconds and 1,000 milliseconds = 1 second)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]`
	`"KeepAliveTime"=dword:6DDD00`
	`"KeepAliveInterval"=dword:000003e8`

Step	Description

	Prevent Windows from 'Hanging' when Users Logs On or Off
	
	The following configuration prevents Windows from 'hanging' when a client logs on or logs off. The Terminal server together with the connected Terminal Services client computers may stop responding or may pause for several seconds.
	
	To address this issue you must turn on the '**Enable advanced performance**' feature for each hard disk that has write caching enabled and that has its write cache protected by battery backup.
	
	From the console destkop right click **My Computer** → and then click **Manage** → click **Device Manager** → click to expand **Disk drives** → right-click the disk drive that you want to configure, and then click **Properties** → click the **Policies** tab → If the Enable write caching on the disk check box is selected, click to select the Enable advanced performance check box → Click **OK**.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters
	Name: MaxWorkItems
	Data Type: DWORD
	Value data: 8196 (decimal)
	
	Name: MaxMpxCt
	Data Type: DWORD
	Value data: 2048 (decimal)
	
	Name: MaxRawWorkItems
	Data Type: DWORD
	Value data: 512 (decimal)
	
	Name: MaxFreeConnections
	Data Type: DWORD
	Value data: 100 (decimal)
	
	Name: MinFreeConnections
	Data Type: DWORD
	Value data: 32 (decimal)
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\Parameters
	Name: MaxCmds
	Data Type: DWORD
	Value data: 2048 (decimal)
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Configuration Manager
	Name: RegistryLazyFlushInterval
	Data Type: DWORD
	Value data: 60 (decimal)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters]`
	`"MaxWorkItems"=dword:00002004`
	`"MaxMpxCt"=dword:00000800`
	`"MaxRawWorkItems"=dword:00000200`
	`"MaxFreeConnections"=dword:00000064`
	`"MinFreeConnections"=dword:00000020`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\Parameters]`
	`"MaxCmds"=dword:00000800`
	`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Configuration Manager]`
	`"RegistryLazyFlushInterval"=dword:0000003c`
	
	Important! You will want to add the above settings to any file servers users connect too.
	
	For more information please visit: http://support.microsoft.com/?kbid=324446

2. 7. Printing Tweaks

The following details tweaks and configurations for the Windows Printing subsystem. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Changing the Default Spool Directory
	
	The following registry tweak will allow you to move the Print Spooler Directory to a directory and disk that contains the freest space. It is also recommended to move the directory to another partition to offload some disk activity from the primary OS drive.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers
	Value Name: DefaultSpoolDirectory
	Data Type: REG_SZ
	Value Data: "<Path to printer spool directory">">
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers]`
	`"DefaultSpoolDirectory"="Path to printer spool directory"`

	Disable System Beep While Printing Jobs
	
	The following registry tweak will disable the server from 'beeping' every few seconds when a remote job error occurs on a print server.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print
	Value Name: BeepEnabled
	Data Type: DWORD
	Value Data: 0 = The computer does not beep each time a print job is retried. 1 = The computer beeps each time the job is retried.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print]`
	`"BeepEnabled"=dword:00000000`

	Disable Print Spooler Notification PopUp from being Displayed on the Server Console
	
	The following registry tweak will disable the print spooler from notifying the end-user that their print job has been completed.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers
	Value Name: NetPopup
	Data Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers]`
	`"NetPopup"=dword:00000000`

Step	Description

	Disable Spooler errors from being displayed on the server console
	
	The following registry tweak suppresses spooler error messages from being displayed on the server console.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler
	Value Name: ErrorControl
	Data Type: DWORD
	Value Data: 0 = Display all error messages, 1 to suppress system error messages, 2 to suppress all errors
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler]`
	`"ErrorControl"=dword:00000002`

	Set Citrix Session Printers to be Retained after Logoff
	
	The following registry tweak is worth setting if using "session printers" in a Citrix policy. Without this, all policy created printers are removed when the user logs out. If one of these printers is set as default it will not keep the setting. It also helps with performance as printers do not have to be created at each logon.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Print
	Value Name: DefaultPrnFlags
	Data Type: DWORD
	Value Data: 00800000
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Print]`
	`"DefaultPrnFlags"=dword:00800000`

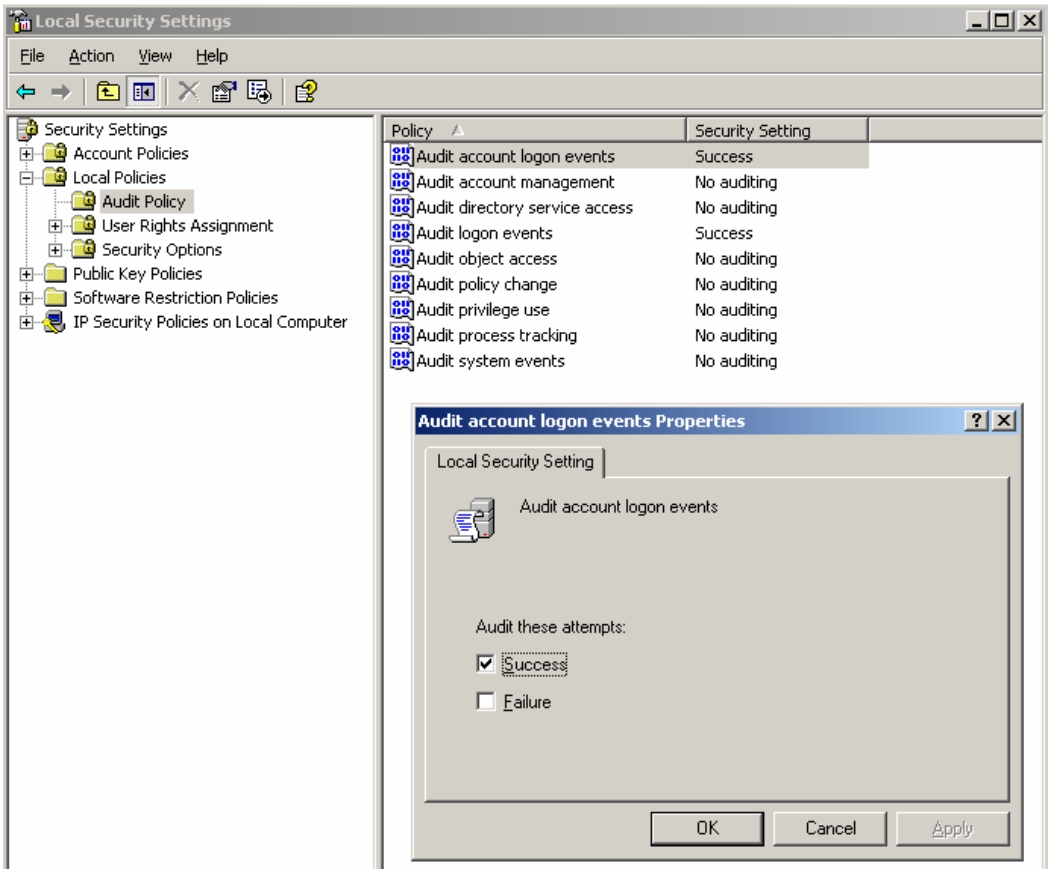
	Disable End-User from Being able to Add or Delete Printers
	
	The following registry tweak prevents end-users from adding new printers and/or deleting their existing ones.
	
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
	Value Name: NoAddPrinter
	Data Type: DWORD
	Value Data: Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Value Name: NoDeletePrinter
	Data Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]`
	`"NoAddPrinter"=dword:00000001`
	`"NoDeletePrinter"=dword:00800001`

Step	Description

	Disable Print Job Logging In Event Log
	
	The following registry tweak suppresses the logging of print jobs in the system event log. Normally Windows logs every print job processed by a server in that machine's application event log. Since for the most part these logs fall into the category of "data no one will ever look at," you can configure the spooler service to not make these log entries in the first place.
	
	To suppress print job event log entries, add a new REG_DWORD value named HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\EventLog and give it a value of 0. As with all the other printing tweaks, this change won't take effect until you stop and restart the Spooler service.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers
	Value Name: EventLog
	Data Type: DWORD
	Value Data: 0 = Disable Logging 1 = Enable Logging
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers]`
	`"EventLog”=dword:00000000`

2. 8. Security Tweaks

The following details tweaks and configurations to secure your Windows Terminal Services server. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description
	Enable Auditing in Local Security Policy The following setting configures security auditing in order to allow you to verify successful and unsuccessful logins and system events. Click the **Start** button → click **Settings** → click **Control Panel** → click **Administrative Tools** → click the **Local Security Policy** applet → click to expand the **Local Policies** node → click the **Audit Policies folder** → Select the Success/Failure events you want to audit. • **Audit Account Logon Events**: Success and Failure • **Audit Logon Events**: Success and Failure • **Audit System Events**: Failure 

Step	Description

	Clear the Last User's Name that Logged on to Windows from the Login Box
	
	The following registry tweak clears the last person's name that logged into the server farm, from the username field of the Microsoft Client.
	
	HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/system
	Value Name: DontDisplayLastUserName
	Data Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/system]`
	`"DontDisplayLastUserName"=dword:0000001`

	Restrict Users Access to the Console's Floppy and CD-ROM Drives
	
	The following registry tweak restricts end-user access to the console's Floppy and CD-ROM drives.
	
	HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\Winlogon
	Value Name: AllocateFloppies
	Data Type: REG_SZ
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Value Name: AllocateCDRoms
	Data Type: REG_SZ
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\Winlogon]`
	`"AllocateFloppies"="1"`
	`"AllocateCDRoms"="1"`

	Display Legal Notice before Login
	
	The following registry tweak displays a legal notice popup dialog box to all users before they log in.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
	Value Name: LegalNoticeCaption
	Data Type: REG_SZ
	Value Data: "Notice Text"
	
	Value Name: LegalNoticeText
	Data Type: REG_SZ
	Value Data: "Caption Text:"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]`
	`"LegalNoticeCaption"="Warning:"`
	`"LegalNoticeText"="Access to this computer system and associated network, computer resources, or data is restricted to those authorized by <YOUR COMPANY>. This computer and related networks, resources or data may only be used for business purposes of <YOUR COMPANY>. and its customers. Use by unauthorized individual or for an unauthorized purpose is a violation of Federal and/or state law. Violators will be prosecuted."`

2. 9. Windows Desktop and Windows Subsystem Tweaks

The following details tweaks and configurations for the Windows Desktop and miscellanies Windows subsystems. This is in no way a conclusive list and not all tweaks apply in all circumstances.

Step	Description

	Configure the Server to Recover from a System Crash
	
	The following registry tweak allows you to specify what happens when the system locks, fails, or terminates abnormally. It consist of the following five sub keys.
	
	• **AutoReboot** specifies whether the system restarts automatically after it fails or locks.
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
	Value Name: AutoReboot
	Data Type: DWORD
	Value Data: 0= Do not restart automatically, 1= Restart automatically.
	
	• **CrashDumpEnabled** specifies whether Windows Server 2003 writes the contents of the system memory to a log file when the system stops unexpectedly. The contents of this log file can be useful in determining why the system stopped.
	Value Name: CrashDumpEnabled
	Data Type: DWORD
	Value Data: 0= Debugging information is not written to a file, 1= Complete crash dump is written to a file, 2= Kernel memory dump is written to a file, 3= Small memory dump is written to a file.
	
	• **LogEvent** specifies whether the system writes an error to the System Log in Event Viewer when Windows Server 2003 terminates abnormally.
	Value Name: LogEvent
	Data Type: DWORD
	Value Data: 0 = No events are logged when the system terminates abnormally, 1 = The system writes an error message to the System Log when the system terminates abnormally.
	
	• **Overwrite** specifies whether the system writes over the old recovery file or creates a new recovery file each time the system stops abnormally.
	Value Name: Overwrite
	Data Type: DWORD
	Value Data: 0 = The system creates a new recovery file for each abnormal stop. This value preserves a record of previous abnormal stops to aid your investigation into the cause of the stops, 1 = The system overwrites the existing recovery file. This value prevents the system from accumulating unused recovery files.
	
	• **SendAlert** specifies whether the system alerts administrators of the computer when the system stops unexpectedly.
	Value Name: SendAlert
	Data Type: DWORD
	Value Data: 0 = The system does not alert administrators when the system stops, 1 = The system alerts administrators when the system stops.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]`
	`"AutoReboot"=dword:00000001`
	`"CrashDumpEnabled"=dword:00000002`
	`"LogEvent"=dword:00000001`
	`"Overwrite"=dword:00000001`
	`"SendAlert"=dword:00000001`
	`"NMICrashDump"=dword:00000001`

Step	Description

	Set the Default Path to the Windows source files
	
	The following registry tweak sets the default location where the OS can find the Windows source files.
	
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup
	Value Name: SourcePath
	Data Type: REG_SZ
	Value Data: "full path to source files" - for example "D:\I386"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup]`
	`"SourcePath"="<full path to source files"`

	Disable Dr Watson
	
	The following registry tweak disables Dr. Watson. It is used to help detect, decode and log errors that are encountered while windows or windows programs are running. In a Terminal Server environment it might be recommend disabling this logging.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
	Value Name: AeDebug
	Data Type: REG_SZ
	Value Data: "Debugger"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]`
	`"Debugger"=""`

	Disable Media Sensing
	
	The following registry tweak controls the Windows "Media Sensing" feature. You may use this feature to detect whether your network media is in a "link state." If there is no link, it disables the interface. This may not be a desirable result on a multi-user server.
	
	Note If you disable the "Media Sensing" feature, you may experience problems. For example, if you have a computer that has two network adapters and you disable the "Media Sensing" feature, if one network adapter does not work, it is unbound. Additionally, if a default gateway is configured, associated routes are removed so that all traffic goes through the other network adapter.
	
	For more information please visit: http://support.microsoft.com/kb/q239924/
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
	Value Name: DisableDHCPMediaSense
	Data Type: DWORD -Boolean
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]`
	`"DisableDHCPMediaSense"=dword:00000001`

Step	Description

	Disabling CD-ROM Autorun Feature
	
	The following registry tweak allows you to disable the CDROM autorun feature. By default, Windows Server 2003 examines inserted CD-ROMs and runs the autorun program.
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom
	Value Name: Autorun
	Value Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom]`
	`"Autorun"=dword:00000001`

	Increase the Size of the Icon Cache
	
	The following registry tweak allows you to increase the size of the Windows Icon Cache. If your Terminal Server has a large amount of applications installed then you might run out of space for Windows to cache the icons. If this occurs it is possible that some icons will be displayed incorrectly.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
	Value Name: Max Cached Icons
	Value Type Type: REG_SZ
	Value Data: The number of icons you wish to cache - maximum 2000 (2000=2MB)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]`
	`"Max Cached Icons"="4096"`

	Speedup Application Load Times
	
	The following registry tweak has the ability to speed up application load times by pre-loading commonly used files. This does require additional memory so it might not be a good tip for memory staved systems.
	
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
	Data Name: EnablePrefetcher
	Data Type: DWORD
	Value Data: 0 = disabled, 1 = application launch prefetching, 2 = boot prefetching, 3 = application and boot prefetching
	
	Note: To clear the prefetcher cache you will need to delete any files located in the \Windows\Prefetch directory.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management\PrefetchParameters]`
	`"EnablePrefetcher"="3"`

Step	Description

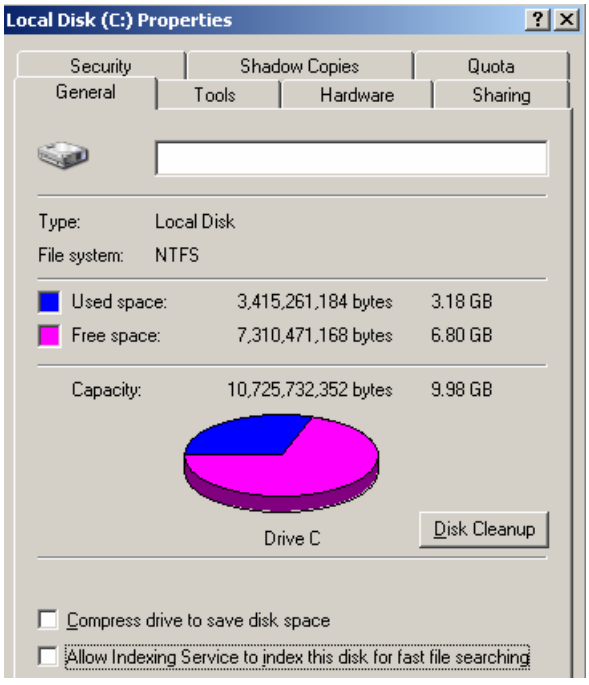
	Set Windows Desktop to use the Classic Start Menu
	
	The following registry tweak configures Windows to use the classic Start Menu.
	
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
	Value Name: NoSimpleStartMenu
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]`
	`"NoSimpleStartMenu"=DWORD:00000001`

	Disable Roaming Profile Cache
	
	The following registry tweak configures Windows to delete the local user profile when they log off. This helps save disk space as it prevents hundreds of profiles from being cached on each Terminal Server. .
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
	Value Name: DeleteRoamingCache
	Data Type:DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]`
	`"DeleteRoamingCache"=dword:00000001`

	Disable Automatic Network Shortcut Resolution
	
	The following registry tweak resolves the potential issue where a shortcut points to the incorrect location. The issue is that Windows Explorer stores not only a drive indicator (N:\Dir\App.exe) but a UNC (\\server\share\app.exe) indicator in each shortcut file. If your copied shortcuts seem to point to their original location instead of to the drive letter shown then fix is for you.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer
	Value Name: LinkResolveIgnoreLinkInfo
	Data Type: DWORD
	Value Data: Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]`
	`"LinkResolveIgnoreLinkInfo"=dword:00000001`

Step	Description

	Remove the Popup Tooltips for the Minimize, Maximize and Close Buttons
	
	The following registry tweak removes the tooltips popup from being shown when a users hovers their mouse over the top right Minimize, Maximize and Close buttons.
	
	HKEY_CURRENT_USER\Control Panel\Desktop
	Value Name: MinMaxClose
	Value Type: REG_SZ
	Value Data: Value: 0
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Control Panel\Desktop]`
	`"MinMaxClose"="0"`

	Disable the File Indexing Service The following tweak will allow you to turn off Windows file indexing. To make searching your hard drive faster Server 2003 keeps a record of all the files on the hard drive. The downside to this is it will slow down normal file commands such as open, close. 1. From **My Computer** right click on the hard drive you wish to disable indexing on and click **Properties**. 2. At the bottom of the drives properties windows click to uncheck the **Allow Indexing Service to index this disk for fast file searching** checkbox and click **OK**.  3. Click **OK** to apply the change to all folders and subfolders. 4. Repeat the above steps for each drive.

Step	Description

	Configure Windows to Unload Unused DLLs from Memory
	
	The following registry tweak allows you to unload DLLs that are not being used. Windows Explorer can cache DLL files in memory for a length of time after they have finished being used. This results in giant amounts of memory being taken up by DLL files that are not even in use.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
	Value Name: AlwaysUnloadDLL
	Value Type: REG_SZ
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]`
	`"AlwaysUnloadDLL"="1"`

	Disable The Notification Area Balloon Tips
	The following registry tweak allows you to disable the notification area balloon tips from appearing in a user session.
	
	Value Name: EnableBalloonTips
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]`
	`"EnableBalloonTips"=dword:00000000`

	Disable Balloon Tips on Start Menu Items
	
	The following registry tweak disabled Windows from presenting you with a start menu balloon tip when you hover the cursor over the Start menu, a Start menu item, or over a notification area icon.
	
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
	Value Name: NoSMBalloonTip
	Value Type: DWORD
	Value Data: 0 = Disabled, 1 = Enabled
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]`
	`"NoSMBalloonTip"=DWORD:00000001`

Step	Description

.	**Disable Console System Popup Messages**
	
	The following registry tweak suppresses system error messages from appearing on the system console. This is extremely important in a Terminal Server environment as there is not always someone click to accept and close the error messages.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows
	Value Name: ErrorMode
	Data Type: DWORD
	Value Data: 0 = All messages are visible, 1 = Only system messages are invisible, 2 = All messages are invisible.
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows]`
	`"ErrorMode"=dword:00000002`

	Set Event Log to Retention and Maximum Log Size
	
	The following registry tweak allows you to configure if the Event Log's retention method and log size. The same value name, data type, and value data is used for all three events logs.
	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System
	Value Name: MaxSize
	Data Type: DWORD
	Value Data: 0x10000–0xFFFF0000 (bytes, in 64 KB increments) (64 KB–4 GB)
	
	Value Name: Retention
	Data Type: DWORD
	Value Data: 0 = Overwrite as needed, 4294967295 = Do not overwrite, The number of days you wish to retain events for, multiplied by 86400 (the number of seconds in one day)
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application]`
	`"MaxSize"=dword:00200000`
	`"Retention"=dword:00000000`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security]`
	`"MaxSize"=dword:00200000`
	`“Retention"=dword:00000000`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System]`
	`"MaxSize"=dword:00200000`
	`“Retention"=dword:00000000`
	
	Note*:* On Windows 2000 the Evntlogs had a standard size of only 512 KB and didn't overwrite as needed, in that case you had to tweak the settings in order to have Eventlogs that really logged something. As a Terminal Server generates a lot of events you need a bigger Eventlog to look back a couple of days.
	
	As per Windows 2003 the Eventlogs have a standard setting of 16 MB and are set to overwrite as needed, in most cases there is no need to change these settings.
	You can do a lot in Eventlog management, but the most important thing is to prevent the Eventlog from being overcrowded by Printevents, that will be in a different group in this forum.

Step	Description

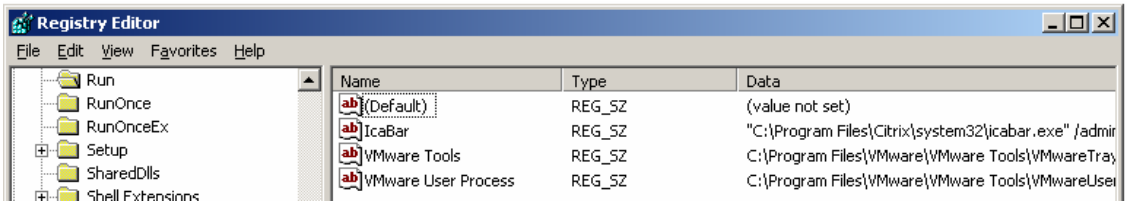
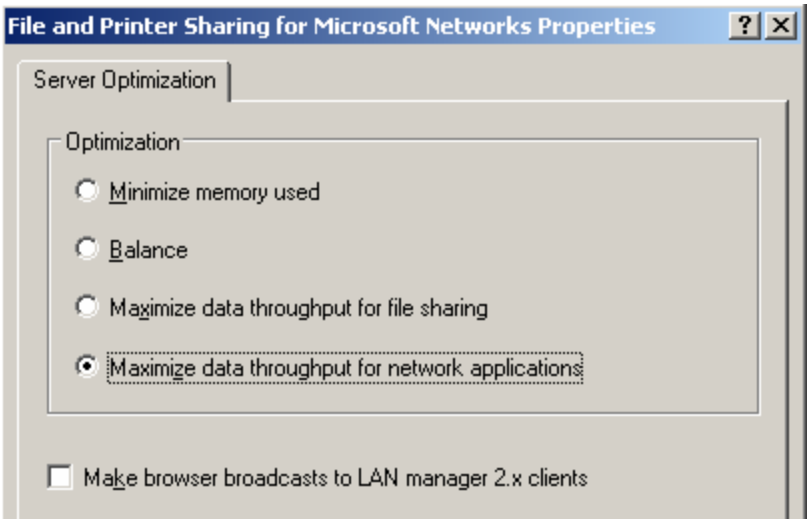
	Set the Name of the My Computer Icon to the Current User and Machine Name
	
	The following registry tweak sets the text of the "My Computer" desktop icon to read, "<username> on <computer name>" This comes in helpful when deploying Terminal Server / Citrix desktop and can be a very useful tool if the user contacts the help desk.
	
	 
	
	HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}]`
	`@="My Computer"`
	`"InfoTip"="Displays the files and folders on your computer"`
	`"LocalizedString"=hex(2):25,00,55,00,53,00,45,00,52,00,4e,00,41,00,4d,00,45,00,\`
	`  25,00,20,00,6f,00,6e,00,20,00,25,00,43,00,4f,00,4d,00,50,00,55,00,54,00,45,\`
	`  00,52,00,4e,00,41,00,4d,00,45,00,25,00,00,00`

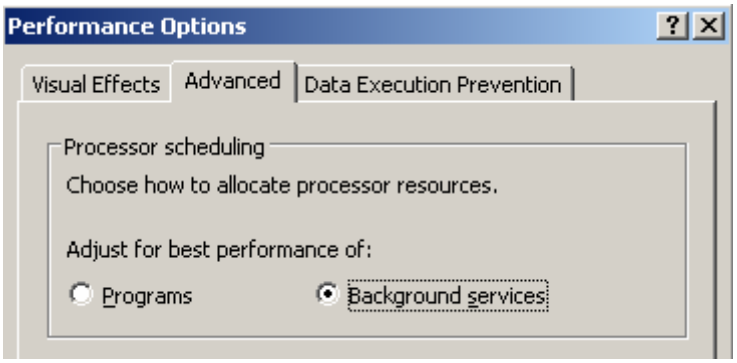
	Disable Caching Recent Documents
	
	The following registry tweak disables Windows from caching the recently accessed documents. Even if the Documents folder has been removed from the Start menu, this process still occurs if not disabled.
	
	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
	Value Name: NoRecentDocsHistory
	Value Type: DWORD
	Value Data: 0 = Enable history, 1 = Disable history
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]`
	`"NoRecentDocsHistory"=dword:00000001`
	
	Note: This registry key can be set per user and/or per server. To configure it per-user please use the HKEY_Current_User key. To configure per server please use the HKEY_Local_Machine key.

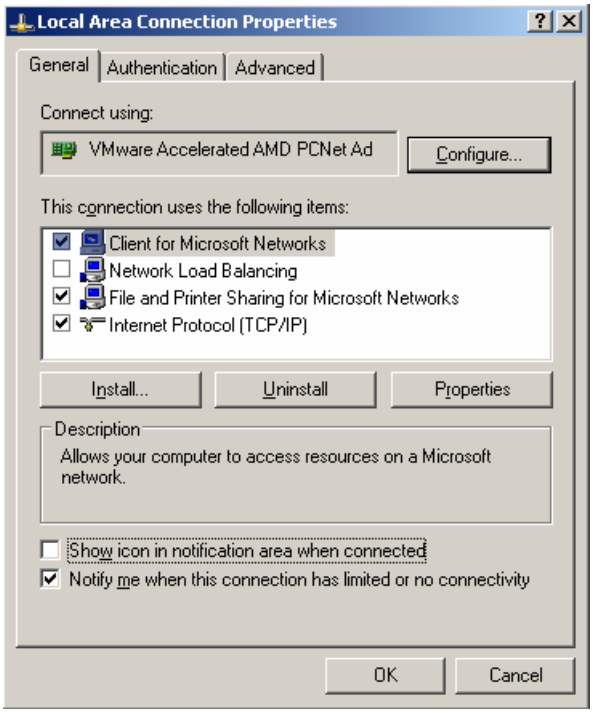
Step	Description

	Enable Windows Classic Style Search
	The following registry tweaks allows you to enable the classic style Windows Search box.
	
	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
	Value Name: Use Search Asst
	Value Type: REG_SZ
	Value Data: "no"
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState]`
	`"Use Search Asst"="no"`

	Password Expire Warning
	The following registry tweak specifies how long before a password expires that the system prompts the user to change the password.
	
	When using a FAT client, logging on to a Citrix session, it can be handy to decrease the Password Expire Warning notice on the Citrix Server. Otherwise users logging on get a expire notice twice.
	
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
	Value Name: passwordexpirywarning
	Value Type: DWORD
	Value Data: 0x0–0xFFFFFFFF days
	
	Recommended .reg file text:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]`
	`“passwordexpirywarning"=dword:00000005`

Step	Description
	Remove Unnecessary Applications From Running in each Session The following allows you to remove unnecessary applications from being executed each time a user logs in. Through the process of installing Windows, Citrix and applications you will find that you tend to collect a fair amount of applications that execute upon a user login. Such applications as the Adobe Acrobat Helper, Antivirus agents, the Citrix ICA Bar and many more. It is recommended to remove the applications that are just not needed. There is no science to this as every system is different but here are just a few examples: Examples: ICABAR.EXE (MetaFrame administrator toolbar) NWTRAY.EXE (Netware tray application) HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\Run 
	Optimize the File System Cache For servers with less than 2GB of physical memory installed it is recommend to configure the file system cache to optimize itself for network related applications. This setting is better for application servers and those with internal memory management features. Click the **Start** button → click **Settings** → click **Control Panel** → click **Network and Dial-Up Connections** → click **Local Area Network** → click the **Properties** button → double click **File and Print Sharing for Microsoft Networks** → click to select the **Maximize Throughput for Network Applications** radio button and click **OK** to save the setting and finish. 

Step	Description
	Optimize Processor Scheduling for a Equal CPU Timeslice The following configuration allows you to configure how long individual threads are allowed to execute on the CPU before a context switch occurs and a new thread is processed. By default, Windows is optimized for foreground application. This allows the server applications to gain more of the CPU's time. In a Terminal Server world this is not recommend as we want all applications to share the CPU equally. Click **Start** → click **Settings** → click **Control Panel** → click the **System** applet → click the **Advanced** tab → click the **Settings** button in the Performance section → click the **Advanced** tab → then click the **Background services** radio button found in the "Processor Scheduling" section. 
.	**Disable OS2 and POSIX Subsystems** The following registry tweak allows you to disable the OS2 and Posix subsystems. If you do not have a need for these, disabling them can free up an incremental amount of server resources. Be sure you aren't using any OS2 or POSIX apps before proceeding since they won't run To disable these subsystems, remove the following keys under Delete the following registry entry. HKEY_LOCAL_MACHINE \System\CurrentControlSet\Control\Session Manager\Subsystems] Value Name:Posix Data Type: REG_EXPAND_SZ Value Data: %SystemRoot%\system32\psxss.exe

Step	Description
	Reduce ICA Traffic by Disabling the Windows Network Status Icon In Windows 2003 Server there is an available option to show the network icon in the system tray. When this option is selected, a network icon is displayed in the system tray within the session, and this network icon blinks each time network traffic occurs. Because the network icon blinks for each update, an infinite feedback loop occurs. When the network icon in the system tray blinks, it causes the ICA session to update, and because the ICA session is being updated, network traffic occurs which causes the network icon to blink, thus causing the infinite loop. Click the **Start** button → click **Settings** → click **Control Panel** → click the **Network Connections** applet → right click the **Local Area Connection** icon and click **Properties**. . 

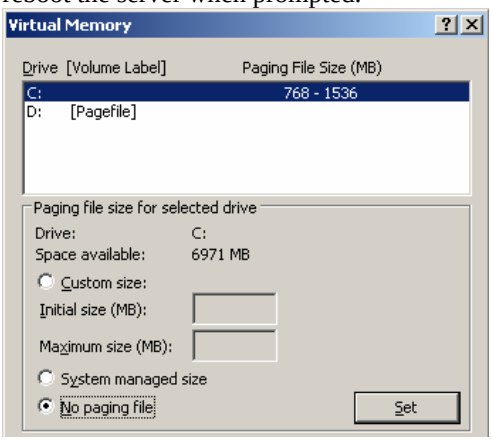
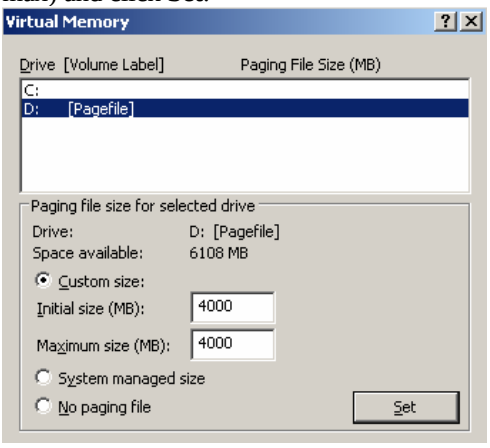
Step	Description
	Disable Unnecessary Windows Services It is recommended to disable any unnecessary Windows Services. The following table details Windows Services that you may wish to modify:

Windows Service Name	Recommend Setting
Application Management	Manual
Alerter	Disabled
Computer Browser	Disabled
Distributed file system	Disabled
Distributed link tracking client	Disabled
Distributed transaction coordinator	Disabled
Error Reporting Service	Disabled
Fax Service	Manual
File Replication	Manual
Help and Support	Disabled
HTTP SSL	Disabled
License Logging	Manual
Messenger	Disabled
Portable Media Serial Number Service	Manual
Shell Hardware Detection	Disabled
Windows Audio	Disabled
Wireless Configuration	Disabled

	Implement any Citrix Security Bulletins It is recommended to verify all Citrix Security Bulletins. A complete list of Citrix Security Bulletins can be found at: http://support.citrix.com/latestsecurityall!execute.jspa.

Step	Description
	Rename the 'Local Administrator' Account It is recommended to rename the local administrator account as this is the first place a hacker starts when attempting to break into a server. It is also important to prevent people from using this account for auditing purposes as if everyone was using the same administrator account then you loose the ability for admin accountability.
	Install Any Remaining Microsoft Critical Updates via Windows Update For security and stability reasons you will want to verify the system is at the latest Microsoft Windows service pack and Hotfix levels. This can be done through numerous methods. The following are just a few tools to ease in this process. Microsoft Windows Update Services http://www.microsoft.com/windowsserversystem/updateservices/default.mspx Microsoft Windows Update http://update.microsoft.com RES Wisdom http://www.realenterprisesolutions.com Microsoft Systems Management Services (SMS) http://www.microsoft.com/smserver/default.mspx

	Defrag System Hard Drives
	
	Run disk defragmentation software on all server drives. Defragmentation is a process that eliminates fragmentation in file systems. It does this by physically reorganizing the contents of the disk in order to store the pieces of each file in order while creating more continuous free space for future files. This is extremely important as once you finish installing Microsoft Windows, Citrix MetaFrame Presentation Server and the applications you system will become very fragmented, thus slowing down file read and write access. Due to the very dynamic aspect of a Terminal Server, disk defragmentation should be run as often as possible.
	
	Note: Before you defrag the server's hard drives you will want to empty the Recycle Bin to clear up free space so it can be properly organized during the defragmentation process.
	
	Example Script: The following script defrags all hard drives on a server. I recommend adding it to the server and running it through a "Scheduled Task".
	
	`'defrag.vbs Defrags all hard disks - This can be run as a Scheduled Task`
	
	`Set WshShell = WScript.CreateObject("WScript.Shell")`
	`Dim fso, d, dc`
	`Set fso = CreateObject("Scripting.FileSystemObject")`
	`Set dc = fso.Drives`
	`For Each d in dc`
	`If d.DriveType = 2 Then`
	`Return = WshShell.Run("defrag " & d & " -f", 1, TRUE)`
	`End If`
	`Next`
	`Set WshShell = Nothing`

Step	Description
	Configure the Server Pagefile for Optimum Performance The following defines how to tune the pagefile for optimum performance. 1. Click the **Start** button → click **Settings** → click **Control Panel** → double click the **System** applet → click on the **Advanced** tab → click the **Settings** button in the Performance box → click the **Advanced** tab → and click the **Change** button. 2. Click to select the drive hosting the current page file and then clear the **Initial size** and **Maximum size** text boxes → click to select the **No Paging File** radio button → Click the **Set** button and then reboot the server when prompted.  3. Once the server has been rebooted, ignore any error messages and defrag the system as documented above. This will create a volume with enough continuous space to prevent against a fragmented pagefile. 4. Return to the **Virtual Memory** window and select the drive you wish to create the pagefile on. If you have multiple physical drives then you will want to select the drive that is the least busy and/or fastest. If you only have disks configured as RAID 1, then you will want to place the Pagefile on it as it will be the fastest drive. 5. Set the PAGEFILE to 2.5 times the total amount of physical RAM installed on the server (4095 MB max) and click **Set**.  Click **OK** to save the new page file and reboot the server when prompted.

Step	Description
	Remove Unwanted Applications Shortcuts from Programs Group You will now want to clean up the Programs Group by removing any unwanted application shortcuts. For example, Outlook Express, Address Book, and many more. Remove any unwanted shortcut from: • C:\Documents and Settings\All Users\Start Menu\Programs • C:\Documents and Settings\Default User\Start Menu\Programs • C:\Documents and Settings\Default User.*domain_name*\Start Menu\Programs
	Cleanup Any Miscellaneous Event Log Error Messages We are now on the last step of installing and configuring Microsoft Windows Server 2003 with Citrix Presentation Server 4.0. This being the case it is recommended to verify and clean up any miscellaneous Event Log error messages that might be logged.