Technical Whitepaper

Most Important Terminal Server Registry Keys and Values

May 2005

Dr. Bernhard Tritsch

Web: http://drtritsch.com

Twitter: @drtritsch

1 Contents

2 Introduction

The relevant configuration options for terminal servers, terminal server sessions, users, and RDP clients can be found in different places in the registry. Administration tools and Group Policies usually change several registry values. The following chapters of this whitepaper provide you with information on their names, paths and default values.

NOTE: This whitepaper provides a general overview of those registry keys that are essential for Terminal Services. A full documentation of all relevant keys would probably be a book in its own right. However, if you know where to find the interesting locations, there is nothing to prevent you from doing your own experiments on a test system. Experiments have produced many tips for optimizing system performance by modifying the registry. However, it is clearly neither advisable nor recommended to tweak the registry settings on a production system.

DISCLAIMER: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

2.1 Automatic Application and Script Execution

Windows Server 2003 offers the option to configure applications or scripts in the registry using different keys. These scripts run automatically if a certain event occurs. This mechanism can be used to perform initialization tasks required on terminal servers. The following list presents the corresponding keys in detail.

- HKCU \SOFTWARE \Microsoft \Windows \CurrentVersion \Run: Entered programs are executed upon each user logon.
- HKCU \SOFTWARE \Microsoft \Windows \CurrentVersion \RunOnce: Entries made by executable programs are deleted after being processed.
- HKCU \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Windows \Run: Entered programs are executed upon each user logon.
- HKCU \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Windows \Load: Entered programs are executed upon each user logon.
- HKLM \SOFTWARE \Policies \Microsoft \System \Scripts: Usually configured through Group Policies.
- HKU \.DEFAULT \SOFTWARE \Microsoft \Windows \CurrentVersion \Run: Default user is used as a template for new user profiles.
- HKCU \SOFTWARE \Microsoft \Windows \CurrentVersion \Run: Entered programs are executed upon each user logon.
- HKLM \SOFTWARE \Microsoft \Windows \CurrentVersion \RunOnce: Entries made by executable programs are deleted after being processed.
- HKLM \SOFTWARE \Microsoft \Windows \CurrentVersion \RunOnceEx: Entries made by executable programs are deleted after being processed.
- HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Terminal Server \Install \Software \Microsoft \Windows \CurrentVersion \Run: Shadow copy.

- HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Terminal Server \Install \Software \Microsoft \Windows \CurrentVersion \RunOnce: Shadow copy.
- HKLM \SOFTWARE \Policies \Microsoft \Windows \System \Scripts \Startup: Usually configured using Group Policies.

If an application or a script is to be run when a user logs off, the following key is used:

- HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Winlogon \LogoffApp: Lists applications and scripts, separated by commas.
- HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Shutdown \LogoffSetting: Controls what action the system should take when the Log Off command is used (0 - Log off; 1 - Shutdown; 2 - Shutdown and Restart; 3 - Shutdown and Power off)
- HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \Shutdown \ShutdownSetting: Controls what action the system should take when the Shutdown command is used (0 - Log off; 1 - Shutdown; 2 - Shutdown and Restart; 3 - Shutdown and Power off)

3 Terminal Server Registry Settings

3.1 General Settings

One of the central HKLM root hive areas can be found under SYSTEM \CurrentControlSet and SYSTEM \ControlSet00n. The numbered ControlSet001 and ControlSet002 subkeys contain control information that is needed to start and keep Windows Server running. One of these two numbered subkeys is the original; the other is the backup copy. On startup, the system determines which one of the keys is the original and saves the result under HKLM \SYSTEM \Select. The last successful set of control information is saved in HKLM \ SYSTEM \CurrentControlSet. The three sets of control information are for the most part identical, but only one is valid and used by the system.

The HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server hive allows you to configure general settings, just as you can under Terminal Services configuration or Group Policies.

Value Names	Data Type, Default Value	Description
DeleteTempDirsOnExit	DWORD: 0x1	Deletes temporary session directories when the user logs off. Possible values are 0 or 1. Change this value using the *Delete temporary directories on exit* server setting in Terminal Services configuration.
fAllowToGetHelp	DWORD: 0x0	Disables or enables remote assistance on this computer. Possible values are 0 or 1. Usually, this setting is established in the *Remote* tab of the Control Panel's system properties.
fDenyTSConnections	DWORD: 0x0	Allows or denies connecting to Terminal Services. Possible values are 0 or 1.
FirstCountMsgQPeeks SleepBadApp	DWORD: 0xF	Default value of the compatibility flag for applications (See later section in this chapter).
fSingleSessionPerUser	DWORD: 0x1	Each user can be limited to one session to save server resources or facilitate session recovery. Possible values are 0 or 1. Change this value using the *Restrict each user to one session* server setting in Terminal Services configuration.
fWritableTSCCPermTab	DWORD: 0x1	Allows write-protection of the *Permissions* tab in the Terminal Services configuration RDP connection settings. Possible values are 0 or 1.
IdleWinStationPoolCount	DWORD: 0x0	Sessions started in the background are assigned to new users. The default value for this setting is 0. For application servers, you can select different values, which might reduce login times for new user sessions.

Value Names	Data Type, Default Value	Description
Modems With Bad DSR	MULTI_SZ	List of modems that have a problem with Data Set Ready (DSR).
MsgQBadAppSleep TimeInMillisec	DWORD: 0x1	Default value of the compatibility flag for applications (see later section in this chapter).
NthCountMsgQPeeksSleep BadApp	DWORD: 0x5	Default value of the compatibility flag for applications (see later section in this chapter).
PerSessionTempDir	DWORD: 0x1	Each user session receives its own temporary directory. Possible values for this setting are 0 or 1. Change this value using the *Use per session directory* server setting in Terminal Services configuration.
ProductVersion	SZ: 5.2	Version number of the terminal server
SessionDirectoryActive	DWORD: 0x0	Indicates whether the session directory for this server is active. Possible values for this setting are 0 or 1.
SessionDirectoryCLSID	SZ	Class ID, needed by the session directory.
SessionDirectoryExCLSID	SZ	Another class ID that the session directory needs.
SessionDirectoryExpose ServerIP	DWORD: 0x1	Indicates whether the server's IP address is exposed with the activated session directory. Possible values for this setting are 0 or 1.
TSAdvertise	DWORD: 0x1	Indicates whether the server advertises itself as the terminal server. Possible values are 0 or 1.
TSAppCompat	DWORD: 0x1	Indicates whether the system is running in application compatibility mode. Possible values are 0 or 1.
TSEnabled	DWORD: 0x1	Indicates whether basic Terminal Services functions are enabled. Possible values are 0 or 1.
TSUserEnabled	DWORD: 0x0	Indicates whether users can log on to the terminal server. Possible values are 0 or 1.

In addition to individual values, this path holds several subkeys that, in turn, contain keys and values for Terminal Services configuration.

Subkeys	Description
AddIns	Configuration of the redirection of clipboard and client ports (redirector).
AuthorizedApplications	Option to configure a list of applications that can be run on the terminal server.

Subkeys	Description
ClusterSettings	Configuration of the session directory.
DefaultUserConfiguration	All default Terminal Services configuration settings, for example, automatic logon data, time limits, initial program, etc.
Dos	Adjusts DOS shell concerning query of keyboard events.
KeyboardTypeMapping	Adjusts keyboard driver for unusual shortcuts or special hardware.
SysProcs	A list of system programs that run in the system context (0) or in the user context (1).
Utilities	Adjusts the specific commands for the prompt: *Change logon, Change port, Change user, Change winsta, Query appserver, Query process, Query session, Query user, Query winsta, Reset session*, and *Reset winsta*.
VIDEO	Device paths for graphics redirection.
Wds	Configuration of TCP/IP log settings, for example delays, buffer attributes, port number, service name, and so on.
WinStations	Specific configuration for each type of connection and the console session.

3.2 System and User Session Settings

In the second table of the previous chapter, the last keys listed are Wds and WinStation. They play a key role in configuring the RDP protocol and user sessions. Because some keys exist in several hives, they should be explained in more detail. It is impossible to list and explain all keys in this whitepaper, so the following tables show only a selection of the most important configuration options. They can be found in one or more of these registry hives:

- **HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server \Wds \rdpwd**
- **HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server \WinStation \Console**
- **HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server \WinStation \Console \RDP**
- **HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server \WinStation \RDP-Tcp**. The values here are changed through the tool Terminal Services Configuration.

Value Names	Data Type	Description
Callback	DWORD	Set modem callback. This value becomes effective only if you set the *fInheritCallback* flag to 0.
CallbackNumber	SZ	Set a phone number for modem callback. This value becomes effective only if you set the *fInheritCallbackNumber* flag to 0.
ColorDepth	DWORD	Default color-depth setting.

Value Names	Data Type	Description
Comment	SZ	Comment string in the administration tool.
Domain	SZ	Set a default domain name on logon of a user session.
DrawGdiplusSupportLevel	DWORD	Support options for graphics elements output with GDI+.
fAutoClientDrives	DWORD	Connect to client drives upon logon.
fAutoClientLpts	DWORD	Connect to client printers upon logon.
fDisableCam	DWORD	Disable client audio mapping.
fDisableCcm	DWORD	Disable client COM port mapping.
fDisableCdm	DWORD	Disable client drive mapping.
fDisableClip	DWORD	Disable Windows client printer mapping.
fDisableEncryption	DWORD	Disable encryption.
fDisableExe	DWORD	Disable program start upon connection.
fDisableLPT	DWORD	Disable use of printers.
fEnableWinStation	DWORD	Enable remote user sessions.
fForceClientLptDef	DWORD	Use client main printer by default.
fInheritAutoClient	DWORD	Inherit the setting on the terminal server to reset the connec-tion when the connection was ended from another source.
fInheritAutoLogon	DWORD	Inherit the setting on the terminal server to use the client's logon information for automatic logon from another source.
fInheritCallback	DWORD	Inherit the setting on the terminal server that a modem calls back from another source.
fInheritCallbackNumber	DWORD	Inherit on the terminal server the phone number for modem callback from another source.
fInheritColorDepth	DWORD	Inherit the setting on the terminal server for color depth from another source.
fInheritInitialProgram	DWORD	Inherit the setting on the terminal server to start an initial program upon logon from another source.
fInheritMaxDisconnectionTime	DWORD	Inherit on the terminal server the maximum time after which disconnected sessions are ended from another source.
fInheritMaxIdleTime	DWORD	Inherit on the terminal server the maximum idle time for user sessions from another source.

Value Names	Data Type	Description
fInheritMaxSessionTime	DWORD	Inherit on the terminal server the maximum session time from another source.
fInheritReconnectSame	DWORD	Inherit the setting on the terminal server whether a new con-nection can be made only from the same client from another source.
fInheritResetBroken	DWORD	Inherit the setting on the terminal server whether the session is ended upon reaching a session limit or upon disconnection from another source. If you do not set this flag, the session will be simply disconnected.
fInheritSecurity	DWORD	Inherit the security setting on the terminal server.
fInheritShadow	DWORD	Inherit the setting on the terminal server for remote control from another source.
fLogonDisabled	DWORD	Selecting this flag disables logon.
fPromptForPassword	DWORD	Makes entering a password obligatory.
fReconnectSame	DWORD	You can reconnect from the same client only as you did previously. This value becomes effective only if you set the *fInheritReconnectSame* flag.
fResetBroken	DWORD	The session ends when a session limit is reached or the connection is broken. If this flag is not set, the session is simply disconnected. This value becomes effective only if you set the *fInheritResetBroken* flag.
fUseDefaultGina	DWORD	Always use the default Windows component to authenticate users.
InitialProgram	SZ	Initial program that is started when a user logs on. This value becomes effective only if you set the *fInheritInitialProgram* flag.
InputBufferLength	DWORD	Input buffer length for the RDP connection in bytes. Default value = 2048.
KeyboardLayout	DWORD	Set keyboard layout.
MaxConnectionTime	DWORD	Maximum session time in seconds. This value becomes effec-tive only if you set the *fInheritMaxSessionTime* flag to 0.
MaxDisconnectionTime	DWORD	Maximum time in seconds after which disconnected sessions are ended. This value becomes effective only if you set the *fInheritMaxDisconnectionTime* flag to 0.

Value Names	Data Type	Description
MaxIdleTime	DWORD	Maximum idle time in seconds for user sessions. This value becomes effective only if you set the *fInheritMaxIdleTime* flag to 0.
MinEncryptionLevel	DWORD	Set the minimum value of encryption level.
NWLogonServer	SZ	Set a NetWare logon server.
OutBufDelay	DWORD	Maximum waiting time in milliseconds until the output buffer for the RDP connection is emptied.
OutBufLength	DWORD	Output buffer length for the RDP connection in bytes.
Password	SZ	Set a default password when logging on to a user session. The password is encrypted and saved here.
PortNumber	DWORD	Port for network communication using the RDP protocol. Default value = 3398.
Shadow	DWORD	Remote control configuration. This value becomes effective only if you set the fInheritShadow flag to 0. 0: Deny remote control 1: Obtain user permission and interact with the session 2: Do not obtain user permission and interact with the session 3: Obtain user permission and display session 4: Do not obtain user permission and display session
UserName	SZ	Set a default user name for logon to a user session.
WorkDirectory	SZ	Working directory that is set on user logon and initial start of an application.

NOTE: Value names with a leading "f" are so-called flags. Flags are binary values that make a statement true (= 1) or false (= 0).

Additional configuration settings of a rather general nature are done through **HKLM \SYSTEM \CurrentControlSet \Control \Terminal Server \Wds \rdpwd \Tds \tcp**.

Value Names	Data Type, Default Value	Description
InteractiveDelay	DWORD: 0xa	?
OutBufCount	DWORD: 0x6	Number of RDP Output Buffers

Value Names	Data Type, Default Value	Description
OutBufDelay	DWORD: 0x64	RDP Output Buffer Transmission Delay
OutBufLength	DWORD: 0x212	RDP Output Buffer Length
PdClass	DWORD: 0x2	?
PdDLL	SZ	Default value: *tdtcp*
PdFlag	DWORD: 0x4e	?
PdName	SZ	Default value: *tcp*
PortNumber	DWORD: 0xd3d	Standard RDP Port: 3389 (d3d hex)
ServiceName	SZ	Default value: *tcpip*

3.3 Default User Configuration

An area relevant to Terminal Server users is located under **HKLM \Software \Microsoft \Windows NT \CurrentVersion \Winlogon**. It includes the AppSetup key, that defines a special script file called UsrLogon.cmd. This script file is executed along with a possible logon script on startup of each terminal server session. The same location also contains the WinStationDisabled key that either denies (0) or allows (1) new terminal server users to log on, regardless of the protocol.

Value Names	Data Type, Default Value	Description
AllowMultipleTSSessions	DWORD: 0x1	Set if a user may log in to multiple terminal server sessions.
AppSetup	SZ	Commands that are executed after user logon. Default value: *UsrLogon.cmd*.
AutoAdminLogon	SZ	If created and set to 1, this key allows an automatic logon of an administrator. This requires writing the appropriate values in *DefaultUserName*, *DefaultPassword*, and *DefaultDomainName*. On exit and restart, Windows should not ask for a password and automatically show the desktop of the user. It is also important to note that if the *DontDisplayLastUserName* value is enabled, the auto logon feature does not function (see Policies). The additional *ForceAutoLogon* setting must be enabled to stop the tweak from resetting on reboot.

Value Names	Data Type, Default Value	Description
AutoLogonCount	SZ	This setting is used to limit the number of automatic logins, once the limit has been reached the auto logon feature will be disabled and the system will display the standard authentication box. Each time the system is rebooted, the value of *AutoLogonCount* will be decremented by one, until it reaches zero. When *AutoLogonCount* reaches zero, no account will be logged on automatically, the *AutoLogonCount* and *DefaultPassword* key values will be deleted from the registry, and *AutoAdminLogon* will be set to zero.
AutoRestartShell	DWORD: 0x1	Restart shell (*Explorer.exe*) automatically if it was stopped.
CachedLogonsCount	SZ: 10	This value controls the number of allowable cached login attempts when the network domain controller is unavailable.
DefaultUserName	SZ	Stores the user name needed for automatic logon or the last logged in user.
DefaultPassword	SZ	If created, this key may stores the password needed for automatic logon. The password is stored in registry, which means anyone who has access to the machine has access to the password.
DefaultDomainName	SZ	Stores the domain name needed for automatic logon.
ForceAutoLogon	SZ	Normally when a Windows machine is configured to automatically logon to a specified account, users can bypass this and enter alternate account information. This tweak forces the machine to auto logon and to ignore any bypass attempts.
Shell	SZ	Standard shell that is executed when a user logs on. Default value is Explorer.exe, but this may be changed on a Terminal Server.
ShowLogonOption	DWORD: 0x0	If enabled, the start screen asking for Ctrl-Alt-Del is displayed.
ShutdownWithoutLogon	SZ	Defines if the server may be shut down from the start screen without user logon.
WinStationsDisabled	SZ	Either denies (0) or allows (1) new terminal server users to log on, regardless of the protocol. At the command shell, you can modify this value using the *Change logon /enable or Change logon /disable* commands.

Another piece of information needed during logon is related to creating or loading the user profile. HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \ProfileList is accessed during user logon. The keys contain the default paths for a default user (DefaultUser), general user (AllUsers), and individual user profiles. Furthermore, this is the location where you can find a list of all users who have logged on to the system. If a user logs on to the terminal server for the first time, he or she inherits both the normal default user settings and the default values for the terminal server session. They are saved under HKLM \SYSTEM \Current ControlSet \Control \Terminal Server \DefaultUserConfiguration.

3.4 Location of System and Special Folders

The location of system and special folders may be configured through **HKLM \Software \Windows \Software \CurrentVersion\Explorer\User Shell Folders**. This is important information if you want to redirect folders in order to reduce the size of user profiles.

Value Names	Data Type, Default Value	Description
Common AppData	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Application Data
Common Desktop	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Desktop
Common Documents	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Documents
Common Favorites	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Favorites
Common Programs	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Start Menu\Programs
Common Start Menu	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Start Menu
Common Startup	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Start Menu\Programs\Startup
Common Templates	EXPAND_SZ	Default value: %ALLUSERSPROFILE%\Templates

3.5 Printer Settings

Connecting and managing printers for terminal servers is a very complex topic. This fact is also quite evident in the registry. The general configuration of the printers used and the associated driver information are located under HKLM \System \CurrentControlSet \Control \Print.

You will find references to the currently installed printer drivers of the terminal server under HKLM \SYSTEM \ControlSet001 \Control \Print \Environments \Windows NT x86 \Drivers \Version-3 \<Printer name>. This correlates with the files under %SystemRoot% \system32 \spool \drivers \w32x86 \3. The user-specific settings for the printers are located in the registry under HKCU \Printers.

If you do not want to install printer drivers from sources that might not be controllable, you have the option of choosing a binding path. This path is called a "trusted printer driver path". To configure this behaviour, you need to add the following keys in **HKLM \SYSTEM \CurrentControlSet \Control \Print \Providers \LanMan Print Services \servers**.

Value Names	Data Type, Default Value	Description
addprinterdrivers	DWORD	If this value is set to 1, printer drivers may be installed.
LoadTrustedDrivers	DWORD	If you set this registry value to 1, this option is enabled.
TrustedDriverPath	SZ	If *LoadTrustedDrivers* is enabled, the path to the printer drivers can be here in the form \\Server name\Share folder.

It is important that the structure of the \\Server name\Share folder mirrors the %System-Root% \system32 \spool \drivers \w32x86 folder. If all the data was properly entered, printer drivers can be installed only from the predefined source, allowing complete control of the printer drivers used.

3.6 TCP/IP Network Control

Network settings that are relevant to Terminal Servers are located under **HKLM \SYSTEM \CurrentControlSet \Services \Tcpip \Parameters**.

Value Names	Data Type, Default Value	Description
EnableDeadGWDetect	DWORD: 0x1	Determines whether TCP performs dead gateway detection. Dead gateway detection is a TCP feature that identifies gateways that are not operating properly and that switches the computer to a new default gateway. When enabled, any given connection defines a gateway as non-operational (dead) when a packet sent to the gateway must be retransmitted more than half of the number of times specified in the value of the *TcpMaxDataRetransmissions* entry. The connection switches to the next gateway in the list in the *DefaultGateway* or *DhcpDefaultGateway* entries. The system defines a gateway as dead when more than 25 percent of its connections have switched to the next default gateway in the list.

Value Names	Data Type, Default Value	Description
EnablePMTUBHDetect	DWORD: 0x0	Determines whether TCP tries to detect black hole routers during the Path MTU (maximum transmission unit) discovery process. Enabling black hole detection increases the maximum number of times TCP retransmits a given segment. If the value of this entry is 1, TCP recognizes when it has transmitted the same segment several times without receiving an acknowledgement. It reduces the maximum segment size (MSS) to 536 bytes, and it sets the Don't-Fragment bit. If, as a result, receipt of the segment is acknowledged, TCP continues this practice in all subsequent transmissions on the connection. This entry is used only when the Path MTU discovery process is performed, that is, when the value of the *EnablePMTUDiscovery* entry is 1.
EnablePMTUDiscovery	DWORD: 0x1	Determines whether TCP uses a fixed, default maximum transmission unit (MTU) or attempts to detect the actual MTU. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers connecting networks with different MTUs. Fragmentation reduces TCP throughput and increases network congestion. By default, this entry applies to all interfaces. However, the MTU can be reduced for any particular interface by changing the default value of the MTU entry in the subkey for that interface. 0: TCP uses an MTU of 576 bytes for all connections to computers outside the local subnet. 1: TCP attempts to discover the MTU of the path to a remote host.

Value Names	Data Type, Default Value	Description
TcpMaxDataRetransmissions	DWORD: 0x5	Windows provides a mechanism to control the initial retransmit time, and then the retransmit time is self-tuning. The timer for a given segment is doubled after each retransmission of that segment. Using this algorithm, TCP tunes itself to the normal delay of a connection. TCP connections over high-delay links will take much longer to time out than those over low-delay links. By default, after the retransmission timer hits 240 seconds, it uses that value for retransmission of any segment that needs to be retransmitted. This can be a cause of long delays for a client to time out on a slow link. *TcpMaxDataRetransmissions* controls the number of times TCP retransmits an individual data segment (non connect segment) before aborting the connection. The retransmission timeout is doubled with each successive retransmission on a connection. It is reset when responses resume. The base timeout value is dynamically determined by the measured round-trip time on the connection. The valid range of this value is 0 - 0xffffffff.
TCPInitialRtt	DWORD: 0xBB8	This parameter (default value = 3 seconds) controls the initial retransmission timeout used by TCP on each new connection. It applies to the connection request (SYN) and to the first data segments sent on each connection. For example, the value data 5000 decimal sets the initial retransmit time to five seconds. You can only increase the value for the initial timeout. Decreasing the value is not supported, even if the valid range for this value is 0 - 65535 (decimal).