Registry Keys for Terminal Services

Registry Keys for Terminal Services

The relevant configuration options for terminal servers, terminal server sessions, users, and clients can be found in different places in the registry. The administration tools and Group Policies, described in the previous chapters, usually change several registry values. The following section provides you with information on their paths and default values.

Note?This section is 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, just as described in this book.

General Settings

We will first examine those areas of the registry that are vital to the global configuration of the terminal server and its sessions. These areas are located in the HKLM root hive.

One of the central HKLM root hive areas can be found under SYSTEM\CurrentControlSet and SYSTEM\ControlSet00*n*. The numbered ControlSet001 and ControlSet002 subkeys contain control information that is needed to start and keep Windows Server 2003 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.

Note?In the following, we assume that ControlSet001 contains the valid control information used by the system. On your system, it could be ControlSet002.

The HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server hive allows you to configure general settings, just as you can under Terminal Services configuration or Group Policies. Some of the values described here will be discussed in detail later in this chapter.

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 "Compatibility Flags" section later 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.

		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.
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 “Compatibility Flags” section later in this chapter.)
NthCountMsgQPeeksSleepBadApp	*DWORD: 0x5*	Default value of the compatibility flag for applications. (See “Compatibility Flags” section later 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.

SessionDirectoryExCLSID	*SZ*	Another class ID that the session directory needs.
SessionDirectoryExposeServerIP	*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.

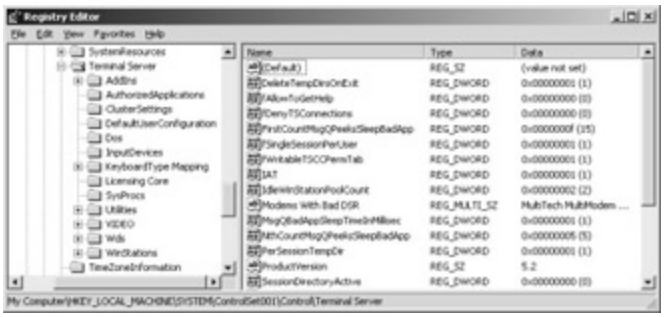

Figure 6-5: Registry values in the HKLM\SYSTEM\ControlSet001\Control\Terminal Server hive. In addition to individual values, this path holds several subkeys that, in turn, contain keys and values for Terminal Services configuration.

Log and User Session Settings

hives, they should be explained in more detail. It is impossible to list and explain all keys in this book, 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\ControlSet001\Control\Terminal Server\Wds\rdpwd
- HKLM\SYSTEM\ControlSet001\Control\Terminal Server\Wds\rdpwd\Tds\tcp
- HKLM\SYSTEM\ControlSet001\Control\Terminal Server\WinStation\Console
- HKLM\SYSTEM\ControlSet001\Control\Terminal Server\WinStation\Console\RDP
- HKLM\SYSTEM\ControlSet001\Control\Terminal Server \WinStation\RDP-Tcp.

  The values here are changed through the tool Terminal Services Configuration.

Table 6.3: The Most Important Subkeys in the HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server Registry Hive

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
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)

	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

Table 6.4 lists the so-called *flags*. Flags are binary values that make a statement true (1) or false (0).

Table 6.4: List of Flags Under HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server \Wds and \WinStations Data Type

Value Names (*DWORD*)	**Description**
fAutoClientDrives	Connect to client drives upon logon.
fAutoClientLpts	Connect to client printers upon logon.
fDisableCam	Disable client audio mapping.
fDisableCcm	Disable client COM port mapping.
fDisableCdm	Disable client drive mapping.
fDisableClip	Disable clipboard mapping.
fDisableCpm	Disable Windows client printer mapping.
fDisableEncryption	Disable encryption.

fDisableLPT	Disable use of printers.
fEnableWinStation	Enable remote user sessions.
fForceClientLptDef	Use client main printer by default.
fInheritAutoClient	Inherit the setting on the terminal server to reset the connection when the connection was ended from another source.
fInheritAutoLogon	Inherit the setting on the terminal server to use the client's logon information for automatic logon from another source.
fInheritCallback	Inherit the setting on the terminal server that a modem calls back from another source.
fInheritCallbackNumber	Inherit on the terminal server the phone number for modem callback from another source.
fInheritColorDepth	Inherit the setting on the terminal server for color depth from another source.
fInheritInitialProgram	Inherit the setting on the terminal server to start an initial program upon logon from another source.
fInheritMaxDisconnectionTime	Inherit on the terminal server the maximum time after which disconnected sessions are ended from another source.
fInheritMaxIdleTime	Inherit on the terminal server the maximum idle time for user sessions from another source.
fInheritMaxSessionTime	Inherit on the terminal server the maximum session time from another source.
fInheritReconnectSame	Inherit the setting on the terminal server whether a new connection can be made only from the same client from another source.

	disconnection from another source. If you do not set this flag, the session will be simply disconnected.
fInheritSecurity	Inherit the security setting on the terminal server.
fInheritShadow	Inherit the setting on the terminal server for remote control from another source.
fLogonDisabled	Selecting this flag disables logon.
fPromptForPassword	Makes entering a password obligatory.
fReconnectSame	You can reconnect from the same client only as you did previously. This value becomes effective only if you set the *fInheritReconnectSame* flag.
fResetBroken	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	Always use the default Windows component to authenticate users.

Table 6.5 lists the most important keys with the *REG_DWORD* data type. These are often directly related to one of the flags listed in the preceding table.

Table 6.5: The Most Important Keys of the *REG_DWORD* under HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server\Wds and *\WinStations* Data Type

Value Names *(DWORD)*	**Description**
Callback	Set modem callback. This value becomes effective only if you set the *fInheritCallback* flag to 0.
ColorDepth	Default color-depth setting.

InputBufferLength	Input buffer length for the RDP connection in bytes. Default value is 2048.
KeyboardLayout	Set keyboard layout.
MaxConnectionTime	Maximum session time in seconds. This value becomes effective only if you set the *fInheritMaxSessionTime* flag to 0.
MaxDisconnectionTime	Maximum time in seconds after which disconnected sessions are ended. This value becomes effective only if you set the *fInheritMaxDisconnectionTime* flag to 0.
MaxIdleTime	Maximum idle time in seconds for user sessions. This value becomes effective only if you set the *fInheritMaxIdleTime* flag to 0.
MinEncryptionLevel	Set the minimum value of encryption level.
OutBufDelay	Maximum waiting time in milliseconds until the output buffer for the RDP connection is emptied.
OutBufLength	Output buffer length for the RDP connection in bytes.
PortNumber	Port for network communication using the RDP protocol. Default value is 3398.
Shadow	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.

Finally, Table 6.6 shows the most important keys of the *REG_SZ* data type.

Table 6.6: The Most Important Keys of the *REG_SZ* under HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server\Wds

CallbackNumber	Set a phone number for modem callback. This value becomes effective only if you set the fInheritCallbackNumber flag to 0.
Comment	Comment string in the administration tool.
Domain	Set a default domain name on logon of a user session.
InitialProgram	Initial program that is started when a user logs on. This value becomes effective only if you set the *fInheritInitialProgram* flag.
NWLogonServer	Set a NetWare logon server.
Password	Set a default password when logging on to a user session. The password is encrypted and saved here.
UserName	Set a default user name for logon to a user session.
WorkDirectory	Working directory that is set on user logon and initial start of an application.

Drivers and Services

The HKLM\SYSTEM\ControlSet001\Services\TermDD hive contains the attributes of the Termdd.sys terminal device driver. However, do not change these attributes. You can find the device driver's path and start option here.

An adjoining hive, called HKLM\SYSTEM\ControlSet001\Services\TermService, hosts both the configuration of Terminal Services within the generic Svchost.exe Windows service and of the Services.exe process. The keys you find there include, for example, the display name, description, complete path, or start options as also listed under services administration. The subkeys show license settings and parameters for the performance indicator object of the system monitor.

Figure 6-6: Drivers and services for terminal server functions.

Note?The UseLicenseServer key under \Parameters is used by Windows NT 4.0, Terminal Server Edition. Windows Server 2003 no longer needs this key. It remains in the registry for compatibility reasons only.

Logon

If you log registry access in a focused manner during logon of a user session, you will gain interesting insights into the corresponding initialization processes. For example, which areas relevant for terminal servers does the Winlogon.exe logon process access?

One piece of information needed during logon concerns creating or loading the user profile. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. These keys contain the default paths for a default user (DefaultUser), general user (AllUsers), and individual user profiles. Furthermore, you can find a list of all users who have logged on to the system here. 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\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server\DefaultUserConfiguration.

Another relevant area 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. (See Chapter 7.) 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. At the prompt, you can modify this value using the **Change logon /enable** or **Change logon /disable** prompts.

The HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\termsrv area is also needed for logon. It defines a specific logic as a response to system events.

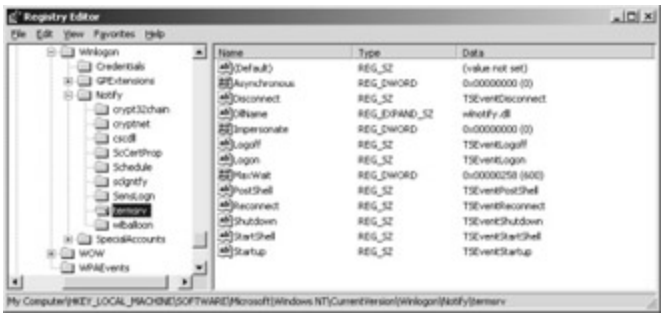

Figure 6-7: Determining the response to system events.

NT\CurrentVersion\Drivers32\Terminal Server\RDP. The video driver configuration plays a certain role for the user session, too. For instance, Explorer.exe needs the corresponding data that is located here: HKLM\SYSTEM\ControlSet001HKLM\SYSTEM\ControlSet001\Control\Terminal Server\VIDEO\rdpdd under the \Device\Video0 key.

If local Group Policies for Terminal Services settings were established, these must be loaded at the right time, of course. This happens during logon with keys found under HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services and the EnableAdminTSRemote key under HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer. However, these areas can be fairly empty if no or just a few local Group Policies were predefined.

Note?Basically, the settings for local Group Policies are located under HKCU\Software\Policies and HKLM\SOFTWARE\Policies. Users have only read-access rights to these two hives. Therefore, Group Policies cannot be modified at the user level.

Printing

Connecting and managing printers for terminal servers is a very complex topic. (See Chapter 4.) 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\WindowsNTx86\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.

Note?Information for the printer drivers for the Windows Server 2003 64 bit versions is located under HKLM\SYSTEM\ControlSet001\Control\Print \Environments\WindowsIA64\Drivers.

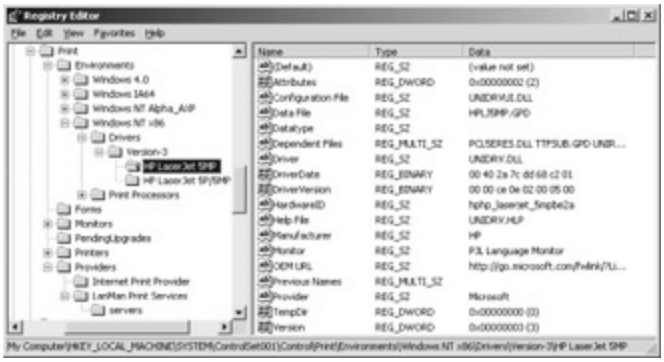

Figure 6-8: Configuring the print environment.

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

- Name: LoadTrustedDrivers; type: REG_DWORD; value: 1
- Name: TrustedDriverPath; type: REG_SZ; value: *Server name*\Share folder

It is important that the structure of the *Server name*\Share folder mirror the %SystemRoot%\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.

User-Specific Configuration

The registry's user-specific section also contains keys that are relevant to the terminal server. For example, the HKCU\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server hive has the key called LastUserIniSyncTime. This key indicates the last system time a user-specific .ini file was synchronized to its corresponding system-wide .ini file (discussed later in this chapter).

If a user has administrator permissions, there is an additional key called TSADMIN here, containing several subkeys. These subkeys allow access to attributes for connection options, alerts, refresh rates, keyboard shortcuts for remote control, server list options, and display values for system processes in the Task Manager.

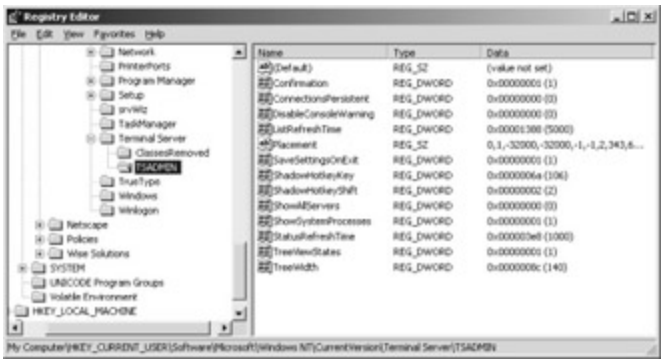

Figure 6-9: User-specific terminal server settings for an administrator.

After a user session has been established, it has its own ID (SESSIONNAME). It is located next to the client name (CLIENTNAME) and the logon server name (LOGONSERVER) in the HKCU\Volatile Environment section of the registry.

Use the following registry sections to define all relevant user folders in which to save data about the applications, desktop, local settings, personal files, network environment, print environment, or start menu:

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Chapter 1: The Concept of Terminal Services

eTutorials.org See also

- Chapter 4: Administration and Operation
- Chapter 5: Integrating Applications
- Chapter 6: Registry
  - The Registry - A Brief Introduction
  - **Registry Keys for Terminal Services**
  - Application-Specific Registry Modifications
  - Compatibility Flags
- Chapter 7: Scripting
- Chapter 8: Security and Stability
- Chapter 9: Citrix MetaFrame XP Presentation Server
- Chapter 10: Administration of Citrix MetaFrame Servers
- Chapter 11: Resource Management in Server Farms
- Chapter 12: Web Access to Terminal Server Applications
- Chapter 13: Application Access Portals
- Chapter 14: Optimization and Troubleshooting
- Chapter 15: How to Plan Production Environments