# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 5, Task ID: 17

| | |
|---|---|
| Task ID: | 17 |
| Risk Level: | 6 |
| Date Processed: | 2016-04-07 08:21:32 (UTC) |
| Processing Time: | 61.24 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\ToggleService32.exe" |
| | |
| Sample ID: | 5 |
| Type: | basic |
| Owner: | admin |
| Label: | ToggleService32.exe |
| Date Added: | 2016-04-07 08:21:31 (UTC) |
| File Type: | PE32:win32 |
| File Size: | 10254 bytes |
| MD5: | 1439e0552127dda0c66b7be1eadb723d |
| SHA256: | 89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a |
| Description: | None |

## Pattern Matching Results

6 Modifies registry autorun entries
6 Writes to system32 folder
2 PE: Nonstandard section
2 Resolves local hostname
6 PE: File has TLS callbacks
3 Program causes a crash [Info]
3 Writes to a log file [Info]
4 Terminates process under Windows subfolder
4 Connects to local IP
3 Long sleep detected
5 Installs service

## Static Events

Anomaly: PE: Contains a virtual section
Anomaly: PE: Contains one or more non-standard sections
Anomaly: PE: File contain TLS callbacks

## Process/Thread Events

Creates process: C:\windows\temp\ToggleService32.exe ["C:\windows\temp\ToggleService32.exe" ]
Creates process: C:\Windows\System32\alg.exe [C:\Windows\System32\alg.exe]
Creates process: C:\Windows\System32\msdtc.exe [C:\Windows\System32\msdtc.exe]
Creates process: C:\Windows\system32\UIODetect.exe [C:\Windows\system32\UIODetect.exe]
Creates process: C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]
Creates process: C:\Windows\System32\spoolsv.exe [C:\Windows\System32\spoolsv.exe]
Creates process: C:\Windows\system32\vssvc.exe [C:\Windows\system32\vssvc.exe]
Creates process: C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -k WerSvcGroup]
Creates process: C:\Windows\system32\svchost.exe [C:\Windows\system32\svchost.exe -k imgsvc]
Loads service: ALG [C:\Windows\System32\alg.exe]
Loads service: AppMgmt [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service: BITS [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service: Browser [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service: TrkWks [C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted]
Loads service: MSDTC [C:\Windows\System32\msdtc.exe]
Loads service: DNSCache [C:\Windows\system32\svchost.exe -k NetworkService]
Loads service: EAPHost [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service: UIODetect [C:\Windows\system32\UIODetect.exe]
Loads service: SharedAccess [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service: PNRPSvc [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]
Loads service: Spooler [C:\Windows\System32\spoolsv.exe]
Loads service: RpcSs [C:\Windows\system32\svchost.exe -k rpcss]
Loads service: SecLogon [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service: SENS [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service: SysMain [C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted]
Loads service: Schedule [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service: LmHosts [C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted]
Loads service: VSS [C:\Windows\system32\vssvc.exe]
Loads service: AudioSrv [C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted]
Loads service: WERSvc [C:\Windows\System32\svchost.exe -k WerSvcGroup]
Loads service: MpsSvc [C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork]
Loads service: STISvc [C:\Windows\system32\svchost.exe -k imgsvc]
Loads service: W32Time [C:\Windows\system32\svchost.exe -k LocalService]

Loads service: WUAUServ [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service: WLANSvc [C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted]
Terminates process: C:\Windows\System32\alg.exe
Terminates process: C:\Windows\System32\VSSVC.exe
Terminates process: C:\Windows\System32\svchost.exe
Terminates process: C:\Windows\Temp\ToggleService32.exe
Creates remote thread: System

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\MSDTC_STATS_EVENT
Creates mutex: \BaseNamedObjects\{1ADD3D63-C272-48DD-BAB4-AE371D1BA179}_S-1-5-19
Creates mutex: \BaseNamedObjects\WIATRACE_MUTEX
Creates event: \BaseNamedObjects\ConsoleEvent-0x0000000000000878
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event: \KernelObjects\MaximumCommitCondition
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\TermSrvReadyEvent
Creates event: \BaseNamedObjects\RouterPreInitEvent
Creates event: \KernelObjects\SystemErrorPortReady
Creates event: \...\WerSvcSystemPermissionsEvent
Creates event: \BaseNamedObjects\WiaServiceStarted

## File System Events

Creates: C:\Windows\SysWOW64\output.txt
Creates: C:\Windows\System32\Msdtc\Trace\dtctrace.log
Creates: C:\Windows\ServiceProfiles\LocalService
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
Creates: C:\ProgramData
Creates: C:\ProgramData\Microsoft
Creates: C:\ProgramData\Microsoft\Crypto
Creates: C:\ProgramData\Microsoft\Crypto\RSA
Creates: C:\ProgramData\Microsoft\Crypto\RSA\
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\2ee7eaf07e5e827fb447b5a5fde32508_c8de13fd-3fba-4ed7-8bab-5bd67d58ec7a
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Creates: C:\Windows\Debug\WIA
Opens: C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\output.txt
Opens: C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\atl.dll
Opens: C:\Windows\System32\wsock32.dll
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\en-US\alg.exe.mui
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\System32\RpcRtRemote.dll
Opens: C:\Windows\Prefetch\MSDTC.EXE-CC1DEC77.pf
Opens: C:\Windows\System32\msdtctm.dll
Opens: C:\Windows\System32\msdtcprx.dll
Opens: C:\Windows\System32\mtxclu.dll
Opens: C:\Windows\System32\clusapi.dll
Opens: C:\Windows\System32\cryptdll.dll
Opens: C:\Windows\System32\resutils.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\bcrypt.dll
Opens: C:\Windows\System32\ktmw32.dll
Opens: C:\Windows\System32\msdtclog.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\xolehlp.dll
Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\Windows\System32\en-US\msdtc.exe.mui
Opens: C:\Windows\System32\comres.dll

Opens: C:\Windows\System32\msdtcVSp1res.dll
Opens: C:\Windows\System32\mtxoci.dll
Opens: C:\Windows\System32\oci.dll
Opens: C:\Windows\system32\oci.dll
Opens: C:\Windows\system\oci.dll
Opens: C:\Windows\oci.dll
Opens: C:\Windows\System32\Wbem\oci.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\oci.dll
Opens: C:\Windows\System32\Msdtc\Trace
Opens: C:\Windows\system32\MSDtc\trace\dtctrace.log
Opens: C:\Windows\System32\secur32.dll
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\Windows\System32\credssp.dll
Opens: C:\Windows\DtcInstall.log
Opens: C:\Windows\System32\Msdtc
Opens: C:\Windows\System32\Msdtc\MSDTC.LOG
Opens: C:\Windows\System32\ntmarta.dll
Opens: C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
Opens: C:\Windows\System32\FirewallAPI.dll
Opens: C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
Opens: C:\Windows\System32\wtsapi32.dll
Opens: C:\Windows\System32\winsta.dll
Opens: C:\Windows\System32\en-US\ui0detect.exe.mui
Opens: C:\Windows\System32\WlSOWndH.dll
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\system32\UIODetect.exe.Local\
Opens: C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac
Opens: C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\System32\duser.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\Windows\System32\xmllite.dll
Opens: C:\Windows\System32\en-US\duser.dll.mui
Opens: C:\Windows\winsxs\amd64_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_106f9be843a9b4e3
Opens: C:\Windows\winsxs\amd64_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_106f9be843a9b4e3\comctl32.dll.mui
Opens: C:\Windows\System32\imageres.dll
Opens: C:\Windows\System32\en-US\imageres.dll.mui
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
Opens: C:\Windows\System32\pnrpsvc.dll
Opens: C:\Windows\System32\userenv.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\Windows\System32\gpapi.dll
Opens: C:\Windows\System32\en-US\svchost.exe.mui
Opens: C:\Windows\System32\wship6.dll
Opens: C:\Windows\System32\IPHLPAPI.DLL
Opens: C:\Windows\System32\winnsi.dll
Opens: C:\Windows\System32\dhcpcsvc6.dll
Opens: C:\Windows\System32\dhcpcsvc.dll
Opens: C:\Windows\System32\sqmapi.dll
Opens: C:\Windows\System32\ssdpapi.dll
Opens: C:\Windows\Temp
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp
Opens: C:\Windows\ServiceProfiles
Opens: C:\Windows\ServiceProfiles\LocalService
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Opens: C:\ProgramData
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\2ee7eaf07e5e827fb447b5a5fde32508_c8de13fd-3fba-4ed7-8bab-5bd67d58ec7a
Opens: C:\Windows\System32\en-US\crypt32.dll.mui
Opens: C:\Windows\System32\ncrypt.dll
Opens: C:\Windows\System32\p2pcollab.dll
Opens: C:\Windows\System32\en-US\p2pcollab.dll.mui
Opens: C:\Windows\System32\QAGENTRT.DLL
Opens: C:\Windows\System32\en-US\QAgentRT.dll.mui
Opens: C:\Windows\System32\en-US\dnsapi.dll.mui
Opens: C:\Windows\System32\fveui.dll
Opens: C:\Windows\System32\en-US\fveui.dll.mui
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\7d15b36cb15a16892c5618e6e123357a.sst
Opens: C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
Opens: C:\Windows\System32\powrprof.dll
Opens: C:\Windows\System32\en-US\spoolsv.exe.mui
Opens: C:\Windows\System32\en-US\setupapi.dll.mui
Opens: C:\Windows\System32\slc.dll

Opens: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Opens: C:\Windows\System32\vssapi.dll
Opens: C:\Windows\System32\vsstrace.dll
Opens: C:\Windows\System32\netapi32.dll
Opens: C:\Windows\System32\netutils.dll
Opens: C:\Windows\System32\srvcli.dll
Opens: C:\Windows\System32\wkscli.dll
Opens: C:\Windows\System32\samcli.dll
Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\virtdisk.dll
Opens: C:\Windows\System32\fltLib.dll
Opens: C:\Windows\System32\en-US\VSSVC.exe.mui
Opens: C:\Windows\System32\en-US\vsstrace.dll.mui
Opens: C:\Windows\System32\samlib.dll
Opens: C:\Windows\System32\es.dll
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\System32\catsrvut.dll
Opens: C:\Windows\System32\mfcsubs.dll
Opens: C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
Opens: C:\Windows\System32\wersvc.dll
Opens: C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Opens: C:\Windows\System32\wiaservc.dll
Opens: C:\Windows\System32\wiatrace.dll
Opens: C:\Windows\debug\WIA\wiatrace.log
Opens: C:\Windows\System32\msv1_0.dll
Opens: C:\Windows\System32\drivers\nwifi.sys
Opens: C:\Windows\AppPatch\drvmain.sdb
Opens: C:\Windows\System32\drivers\ndisuio.sys
Opens: C:\Windows\System32\drivers\etc\lmhosts
Writes to: C:\Windows\SysWOW64\output.txt
Writes to: C:\Windows\System32\Msdtc\Trace\dtctrace.log
Writes to: C:\Windows\System32\Msdtc\MSDTC.LOG
Writes to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\2ee7eaf07e5e827fb447b5a5fde32508_c8de13fd-3fba-4ed7-8bab-5bd67d58ec7a
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Reads from: C:\Windows\SysWOW64\output.txt
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new

## Network Events

DNS query: WPAD
DNS query: WORKGROUP
DNS query: __MSBROWSE__
DNS query: WORKGROUP
Connects to: 10.74.6.255:138
Connects to: 10.74.6.255:137
Sends data to: 10.74.6.255:138
Sends data to: 10.74.6.255:137
Receives data from: 10.74.6.100:138
Receives data from: 10.74.6.100:137

## Windows Registry Events

Creates key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8
Creates key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\control
Creates key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#\control
Creates key: HKLM\system\currentcontrolset\control\deviceclasses
Creates key: HKCU\software\classes\local settings\muicache\16\52c64b7e
Creates key: HKCU\software\classes\local settings\muicache
Creates key: HKLM\system\currentcontrolset\services\umbus\enum
Creates key: HKLM\software\classes
Creates key: HKLM\system\currentcontrolset\services\vss\diag\registry writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\asr writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization writer
Creates key: HKLM\system\currentcontrolset\control\stillimage\trace
Creates key: HKLM\system
Creates key: HKLM\system\currentcontrolset
Creates key: HKLM\system\currentcontrolset\control
Creates key: HKLM\system\currentcontrolset\control\stillimage
Creates key: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll

Creates key: HKLM\system\currentcontrolset\services\nativewifip\enum
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000\control
Creates key: HKLM\system\currentcontrolset\services\nativewifip\parameters
Creates key: HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
Creates key: HKLM\system\currentcontrolset\services\nativewifip
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007
Creates key: HKLM\system\currentcontrolset\services\ndisuio\enum
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000
Creates key: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000\control
Creates key: HKLM\system\currentcontrolset\services\ndisuio
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009
Deletes value: HKLM\system\currentcontrolset\services\umbus\enum[1]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\system\currentcontrolset\control\mui\settings
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\rpc
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
Opens key: HKLM\software\microsoft\com3
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\treatas
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\progid
Opens key: HKCR\wow6432node\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprocserver32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler
Opens key: HKCR\appid\alg.exe
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key: HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\wow6432node\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\wow6432node\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\wow6432node\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\wow6432node\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\wow6432node\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\wow6432node\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\wow6432node\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKCR\wow6432node\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKLM\software\microsoft\alg\isv
Opens key: HKLM\software\microsoft\msdtc\tracing
Opens key: HKLM\software\microsoft\msdtc\tracing\sources
Opens key: HKLM\software\microsoft\msdtc\tracing\output
Opens key: HKLM\software\microsoft\msdtc
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc
Opens key: HKCR\cid.local
Opens key: HKCR\cid.local\1595e9be-2b8c-422b-aee2-89faa800009a
Opens key: HKCR\cid.local\1595e9be-2b8c-422b-aee2-89faa800009a\description
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\description
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\description
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\description
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\description
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\svcid
Opens key: HKCR\svcid.local
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\host
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\clsid
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\protocol
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\endpoint
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\customproperties
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\customproperties\log
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\customproperties\log\size
Opens key: HKLM\software\microsoft\msdtc\mtxoci
Opens key: HKLM\software\microsoft\msdtc\security
Opens key: HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
Opens key: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\customproperties\log\path
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\currentcontrolset\control\timezoneinformation
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules

Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
Opens key: HKLM\software\microsoft\windows nt\currentversion
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\svcid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\host
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\clsid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\protocol
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\endpoint
Opens key: HKCU\control panel\international
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\customproperties
Opens key: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\customproperties\dac
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\svcid
Opens key: HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\host
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\clsid
Opens key: HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\protocol
Opens key: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\endpoint
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\svcid
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\host
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\clsid
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\protocol
Opens key: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\endpoint
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKU\.default\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop\languageconfiguration
Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\control panel\desktop\muicached
Opens key: HKU\.default\control panel\international
Opens key: HKLM\software\microsoft\ctf\compatibility\ui0detect.exe
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\ctf\knownclasses
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\directui
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\localservicepeernet
Opens key: HKLM\system\currentcontrolset\services
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\software\policies\microsoft\peernet
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1-3a1fc5ac
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\software\microsoft\sqmclient
Opens key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp
Opens key: HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
Opens key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag

Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0
Opens key: HKU\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
Opens key: HKCU\environment
Opens key: HKCU\volatile environment
Opens key: HKCU\volatile environment\0
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\microsoft\cryptography\oid
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\#16
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\ldap
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 012
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKLM\system\currentcontrolset\control\deviceclasses
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKCU\software\classes\local settings\muicache\16\52c64b7e
Opens key: HKCU\software\classes\local settings\muicache
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&6373acf&0&400008#{2accfe60-

c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2d9c6e01&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&1#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-84ae-d30803bae505}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-84ae-d30803bae505}\##?#root#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0f03#4&1d401fb5&0#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&2544b901&0&0001#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&d9ecb39&0&0001#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&2544b901&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&d9ecb39&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&0&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&1&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&0&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&0&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&1&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&0&ef#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&1&ef#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-b732-99a6111edc0b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-a5d6-28db04c10000}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-a5d6-28db04c10000}\##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-00a0c9062857}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&1#{4afa3d53-74a7-11d0-be5e-00a0c9062857}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&2#{4afa3d53-74a7-11d0-be5e-00a0c9062857}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&2544b901&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&d9ecb39&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&2544b901&0&0001#{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&d9ecb39&0&0001#{4d1e55b2-f16f-11cf-88cb-001111000030}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&2544b901&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&d9ecb39&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskhitachi_____0.6.5.8_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskvbox_harddisk_____1.0_____#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskwesterndigital_____4.5.1.6_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&3af2ddc5&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&23a61b21&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-rom_____1.0_____#5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&23a61b21&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&28836b88&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-rom_____1.0_____#5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{8063a3d0-8213-11e3-a68e-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{8063a3d0-8213-11e3-a68e-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#00000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#000000046528ec00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{a1c59152-41e6-11e5-9d66-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{a1c59152-41e6-11e5-9d66-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-

806e6f6e6963}#0000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#000000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{f91930d2-41e9-11e5-ba58-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{f91930d2-41e9-11e5-ba58-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot10#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot2#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot4#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot6#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot8#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&1fc3087&0&28f0#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&2e5a831d&0&28f0#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_00000000&rev_00#3&267a616a&0&10#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#root#umbus#0000#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#\control
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a#0#{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-a537-0000f8753ed1}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-0000f8753ed1}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-

b7df-24c5d8a8ccb8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#4&2abfaa30&0&12345678&00&02#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2dcf5eab&0&12345678&06&05#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2fab8e39&0&12345678&06&05#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&2544b901&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&d9ecb39&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_kbd#0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-af1f-0000f800845c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb5&0#{97f76ef0-f883-11d0-af1f-0000f800845c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____x3220__@_2.40ghz#_1#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____x3220__@_2.40ghz#_3#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____x3220__@_2.40ghz#_4#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_44_-_intel(r)_xeon(r)_cpu_____e5620__@_2.40ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_45_-_____intel(r)_xeon(r)_cpu_e5-2430_0_@_2.20ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_58_-_____intel(r)_core(tm)_i7-3615qm_cpu_@_2.30ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_58_-_____intel(r)_core(tm)_i7-3520m_cpu_@_2.90ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34d3cc#{a5dcbf10-6530-11d2-901f-00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#fac72212e15e713#{a5dcbf10-6530-11d2-901f-00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#*isatap#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_l2tpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanbh#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_sstpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#system#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_sstpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-ac88-96b894c191e2}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-ac88-96b894c191e2}\##?#acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4&22939226&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&13571ab5&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&24693ec3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub20#4&211f73e0&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub20#4&305beb51&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-08002be10318}
Opens key: HKLM\system\currentcontrolset\services\umbus
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllencodepublickeyandparameters
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodepublickeyandparameters
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllencodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\system\currentcontrolset\control\print
Opens key: HKCR\clsid
Opens key: HKLM\software\policies\microsoft\windows nt\printers
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key: HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
Opens key: HKCR\appid\vssvc.exe
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprocserver32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\treatas
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler32
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\vss\settings
Opens key: HKLM\system\currentcontrolset\services\vss\diag
Opens key: HKLM\system\currentcontrolset\services\vss\diag\registry writer
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\progid
Opens key: HKCR\wow6432node\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\wow6432node\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\progid
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler
Opens key: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\progid
Opens key: HKCR\wow6432node\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\wow6432node\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\progid
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
Opens key: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKCR\interface\{00000100-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000100-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32

Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler
Opens key: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
Opens key: HKLM\system\currentcontrolset\services\vss\diag\asr writer
Opens key: HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization writer
Opens key: HKCR\interface\{00000000-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000000-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
Opens key: HKLM\system\currentcontrolset\services\wersvc
Opens key: HKLM\system\currentcontrolset\services\wersvc\parameters
Opens key: HKLM\software\microsoft\windows\windows error reporting
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\imgsvc
Opens key: HKLM\system\currentcontrolset\services\stisvc
Opens key: HKLM\system\currentcontrolset\services\stisvc\parameters
Opens key: HKLM\system\currentcontrolset\control\stillimage\trace
Opens key: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
Opens key: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\treatas
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler32
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\progid
Opens key: HKCR\wow6432node\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
Opens key: HKCR\wow6432node\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\progid
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprocserver32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
Opens key: HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKCR\wow6432node\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKLM\system\currentcontrolset\control\stillimage\fakedevices
Opens key: HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
Opens key: HKLM\system\currentcontrolset\control\stillimage
Opens key: HKLM\system\currentcontrolset\control\stillimage\events
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\connected
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\connected\{daead956-ece5-4c3a-bec4-caa012f74090}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\disconnected
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\emailimage
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\faximage
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\printimage
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{daead956-ece5-4c3a-bec4-caa012f74090}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent
Opens key: HKLM\system\currentcontrolset\control\stillimage\serversettings
Opens key: HKLM\system\currentcontrolset\services\nativewifip
Opens key: HKLM\system\currentcontrolset\services\nativewifip\enum
Opens key: HKLM\system\currentcontrolset\enum\root
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
Opens key: HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-0000f8753ed1}
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
Opens key: HKLM\system\currentcontrolset\services\nativewifip\parameters
Opens key: HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0005\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
Opens key: HKLM\system\currentcontrolset\services\ndisuio
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage
Opens key: HKLM\system\currentcontrolset\services\ndisuio\enum
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000
Opens key: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage
Opens key: HKLM\system\currentcontrolset\enum\root*teredo\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage
Opens key: HKLM\system\currentcontrolset\enum\root*isatap\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\linkage
Opens key: HKLM\system\currentcontrolset\control\diagnostics\performance
Opens key: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]
Queries value: HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[bca9f854]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_cm]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_svc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_gateway]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_tip]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_log]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_tm]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[tracefilepath]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[debugoutenabled]
Queries value: HKLM\software\microsoft\msdtc[noparallellogflushnotification]
Queries value:
HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
Queries value: HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\misc[disabletracing]
Queries value: HKLM\software\microsoft\msdtc[disableterminationonheapcorruption]
Queries value: HKLM\software\microsoft\msdtc[sysprepinprogress]
Queries value: HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
Queries value: HKCR\cid.local\1595e9be-2b8c-422b-aee2-89faa800009a\description[]
Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\description[]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\description[]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\description[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\description[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\svcid[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\host[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\clsid[]
Queries value: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\protocol[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-161e26d1b0e2\endpoint[]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-
161e26d1b0e2\customproperties\log\size[]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
Queries value: HKLM\software\microsoft\msdtc\security[accountname]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccess]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
Queries value: HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
Queries value: HKLM\software\microsoft\msdtc\security[xatransactions]
Queries value: HKLM\software\microsoft\msdtc\security[lutransactions]
Queries value: HKCR\cid.local\ef0ded66-0080-487a-981a-
161e26d1b0e2\customproperties\log\path[]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
8bd7-da8f1a74051a]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]

Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[minbuffers]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[buffersize]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[bias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[uniqueid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[active]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[level]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[controlflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-af58-73e332dcac8d]
Queries value: HKLM\software\microsoft\msdtc[dtcmaxsessions]
Queries value: HKLM\software\microsoft\msdtc[donotgoidle]
Queries value: HKLM\software\microsoft\msdtc[disabletippassthrucheck]
Queries value: HKLM\software\microsoft\msdtc[mincheckpointinterval]
Queries value: HKLM\software\microsoft\msdtc[maxcheckpointinterval]
Queries value: HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
Queries value: HKLM\software\microsoft\msdtc\security[snapshotsecuritydisabled]
Queries value: HKLM\software\microsoft\msdtc[servertcpport]
Queries value: HKLM\software\microsoft\windows nt\currentversion[currentversion]
Queries value: HKLM\software\microsoft\msdtc[cmcancelrpcafter]
Queries value: HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
Queries value: HKLM\software\microsoft\msdtc[cmmaxidlepings]
Queries value: HKLM\software\microsoft\msdtc[cmpingfreqsecs]
Queries value: HKLM\software\microsoft\msdtc[cmverbose]
Queries value: HKLM\software\microsoft\msdtc[rpcqoscapabilities]
Queries value: HKLM\software\microsoft\msdtc[rpcqosidentity]
Queries value: HKLM\software\microsoft\msdtc[rpcauthnsvc]
Queries value: HKLM\software\microsoft\msdtc[numcccimhistoryentries]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\svcid[]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\host[]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\clsid[]
Queries value: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\protocol[]
Queries value: HKCR\cid.local\8bbb1b41-c5f0-4542-a331-158eee269140\endpoint[]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\msdtc[notracking]
Queries value: HKLM\software\microsoft\rpc\securityservice[9]
Queries value: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
Queries value: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
Queries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\svcid[]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\host[]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\clsid[]
Queries value: HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\protocol[]
Queries value: HKCR\cid.local\87ade280-fa9b-49fb-abf8-7b3524224461\endpoint[]
Queries value: HKLM\software\microsoft\msdtc[overridetiphostname]
Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\svcid[]
Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\host[]
Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\clsid[]
Queries value: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]

Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\protocol[]
Queries value: HKCR\cid.local\84cac0b1-bcaf-4600-8dc2-440683466968\endpoint[]
Queries value: HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
Queries value: HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
Queries value: HKLM\software\microsoft\msdtc[transactionbridge]
Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
Queries value: HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
Queries value: HKLM\software\microsoft\msdtc[logwarnenabled]
Queries value: HKLM\software\microsoft\msdtc[suppressduplicateduration]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid[]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\software\microsoft\msdtc[supportns]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[ui0detect]
Queries value: HKU\.default\control panel\desktop[preferreduilanguages]
Queries value: HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\svchost[localservicepeernet]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
Queries value: HKLM\software\policies\microsoft\peernet[disabled]
Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
Queries value:

HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries64]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries64]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value: HKLM\software\microsoft\sqmclient[machineid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[seedserver]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[disablemulticastpublish]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[disablemulticastsearch]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[disabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[searchonly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[mincpalifetime]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
19[profileimagepath]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value: HKCU\control panel\international[localename]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[publishexpandedpath]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 012[name]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[image path]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
Queries value: HKLM\software\policies\microsoft\cryptography[forcekeyprotection]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7[name]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#\control[linked]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-

843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\control[referencecount]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&6373acf&0&400008#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2d9c6e01&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&1#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-84ae-d30803bae505}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-84ae-d30803bae505}\##?#root#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0f03#4&1d401fb5&0#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&2544b901&0&0001#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&d9ecb39&0&0001#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&2544b901&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&d9ecb39&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&0&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&1&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&0&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&0&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&1&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&0&ef#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&1&ef#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-b732-99a6111edc0b}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-a5d6-28db04c10000}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-a5d6-28db04c10000}\##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-00a0c9062857}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&1#{4afa3d53-74a7-11d0-be5e-00a0c9062857}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&2#{4afa3d53-74a7-11d0-be5e-00a0c9062857}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&2544b901&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&d9ecb39&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&2544b901&0&0001#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&d9ecb39&0&0001#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&2544b901&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&d9ecb39&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskhitachi_____0.6.5.8_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskvbox_harddisk_____1.0_____#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#diskwesterndigital_____4.5.1.6_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&3af2ddc5&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&23a61b21&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-rom_____1.0_____#5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&23a61b21&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____1.05____#5&28836b88&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-rom_____1.0_____#5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{8063a3d0-8213-11e3-a68e-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{8063a3d0-8213-11e3-a68e-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-806e6f6e6963}#0000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-

806e6f6e6963}#000000046528ec00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-
806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-
806e6f6e6963}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-
806e6f6e6963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{846ee343-7039-11de-9d20-
806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{a1c59152-41e6-11e5-9d66-
806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{a1c59152-41e6-11e5-9d66-
806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#0000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#000000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{d5e2ffe2-f518-11df-a5c1-
806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{f91930d2-41e9-11e5-ba58-
806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{f91930d2-41e9-11e5-ba58-
806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot10#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot2#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot4#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot6#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot8#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
85bb-30ff1f953599}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&1fc3087&0&28f0#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&2e5a831d&0&28f0#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_00000000&rev_00#3&267a616a&0&10#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#root#umbus#0000#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-bcf7-00aa00b7b32a}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a#0#{72631e54-78a4-11d0-bcf7-00aa00b7b32a}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-a537-0000f8753ed1}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-0000f8753ed1}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#4&2abfaa30&0&12345678&00&02#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2dcf5eab&0&12345678&06&05#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2fab8e39&0&12345678&06&05#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&2544b901&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&d9ecb39&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_kbd#0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-af1f-0000f800845c}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb5&0#{97f76ef0-f883-11d0-af1f-0000f800845c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____________x3220__@_2.40ghz#_1#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____________x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____________x3220__@_2.40ghz#_3#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_15_-_intel(r)_xeon(r)_cpu_____________x3220__@_2.40ghz#_4#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_44_-_intel(r)_xeon(r)_cpu_____________e5620__@_2.40ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_45_-_________intel(r)_xeon(r)_cpu_e5-2430_0_@_2.20ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_58_-_________intel(r)_core(tm)_i7-3615qm_cpu_@_2.30ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_intel64_family_6_model_58_-_________intel(r)_core(tm)_i7-3520m_cpu_@_2.90ghz#_0#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34d3cc#{a5dcbf10-6530-11d2-901f-00c04fb951ed}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#fac72212e15e713#{a5dcbf10-6530-11d2-901f-00c04fb951ed}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#*isatap#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_l2tpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanbh#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#ms_sstpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#root#system#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_sstpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-ac88-96b894c191e2}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-ac88-96b894c191e2}\##?#acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4&22939226&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&13571ab5&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&24693ec3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub20#4&211f73e0&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub20#4&305beb51&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[service]
Queries value: HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[classguid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-08002be10318}[lowerfilters]
Queries value: HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[lowerfilters]
Queries value: HKLM\system\currentcontrolset\services\umbus\enum[count]
Queries value: HKLM\system\currentcontrolset\services\umbus\enum[0]
Queries value: HKLM\system\currentcontrolset\services\umbus\enum[1]
Queries value: HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[upperfilters]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-08002be10318}[upperfilters]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[spoolsv]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-8242-e03a18b5be01]
Queries value: HKLM\system\currentcontrolset\control\print[exceptionhandlerenabled]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifymax]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifysleep]
Queries value: HKLM\system\currentcontrolset\control\print[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\print[maxrpccalls]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
Queries value: HKLM\system\currentcontrolset\control\print[callexitprocessonshutdown]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a544a85b]
Queries value: HKLM\software\microsoft\com3[finalizeractivitybypass]
Queries value: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid[]
Queries value: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
Queries value: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid[]
Queries value: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[idletimeout]
Queries value: HKLM\system\setup[upgradeinprogress]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]
Queries value: HKLM\system\currentcontrolset\services\vss\diag[]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid[]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKCR\interface\{00000100-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKCR\interface\{0000000c-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[6851adeb-79da-4250-a440-f1f52d28711d]
Queries value: HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicedllunloadonstop]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
Queries value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[suppressprocessoutput]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[maxfilesize]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracemask]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaultenableobjecttracking]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[heapoptions]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[traceflags]
Queries value:

HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracemask]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracelevel]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[maxtracearraysize]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[heapoptions]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
Queries value: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[authenticationlevel]
Queries value: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[accesspermission]
Queries value: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid[]
Queries value: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[34dba8a7]
Queries value: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[]
Queries value: HKLM\system\currentcontrolset\control\stillimage[deviceid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{daead956-ece5-4c3a-bec4-caa012f74090}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{daead956-ece5-4c3a-bec4-caa012f74090}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{daead956-ece5-4c3a-bec4-caa012f74090}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{daead956-ece5-4c3a-bec4-caa012f74090}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[defaulthandler]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\emailimage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\printimage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[guid]
Queries value:

HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{daead956-ece5-4c3a-bec4-caa012f74090}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{daead956-ece5-4c3a-bec4-caa012f74090}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{daead956-ece5-4c3a-bec4-caa012f74090}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{daead956-ece5-4c3a-bec4-caa012f74090}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[defaulthandler]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelay]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[imagepath]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[objectname]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[type]
Queries value: HKLM\system\currentcontrolset\services\nativewifip\enum[count]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[displayname]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[service]
Queries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[classguid]
Queries value: HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-0000f8753ed1}[lowerfilters]
Queries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[lowerfilters]
Queries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[upperfilters]
Queries value: HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-0000f8753ed1}[upperfilters]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-99ea-fe66a8355df8]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filtertype]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterruntype]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterclass]
Queries value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[imagepath]

Queries value: HKLM\system\currentcontrolset\services\ndisuio[objectname]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[type]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\services\ndisuio\enum[count]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[displayname]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[classguid]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[lowerfilters]
Queries value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[upperfilters]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-aded-5304bf8f636d]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b3eee223-d0a9-40cd-adfc-50f1888138ab]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root*teredo\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root*isatap\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableipsourcerouting]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableaddrmaskreply]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcastarpreply]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablemediasenseeventlog]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablemulticastforwarding]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcptimedwaitdelay]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhdetect]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enabletcpa]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enabledca]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[minimumpacketsizetodma]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableconnectionratelimiting]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[qualifyingdestinationthreshold]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationsubnet]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationmask]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxuserport]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[ipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[subnetmask]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[ipautoconfigurationaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[performrouterdiscovery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[defaultgateway]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[defaultgatewaymetric]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[solicitationaddressbcast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[usezerobroadcast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[typeofinterface]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[mtu]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[interfacemetric]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[tcpackfrequency]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[tcpdelackticks]
Queries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[start]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[flushthreshold]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[buffersize]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[minimumbuffers]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[flushtimer]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[maximumbuffers]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[filename]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[enablekernelflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[stackwalkingfilter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[clocktype]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[maxfilesize]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[logfilemode]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

context logger[disablerealtimepersistence]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[guid]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[filecounter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[filemax]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[pooltagfilter]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-af71-3e63d056f174]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip[nextinstance]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000\control[*newlycreated*]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[service]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[legacy]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[configflags]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[class]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[classguid]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[devicedesc]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip\enum[0]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip\enum[count]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip\enum[nextinstance]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000\control[activeservice]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio[nextinstance]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000\control[*newlycreated*]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[legacy]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[configflags]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[class]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[classguid]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[devicedesc]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio\enum[0]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio\enum[count]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio\enum[nextinstance]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000\control[activeservice]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[ndisminorversion]
Value changes: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#\control[linked]
Value changes: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\control[referencecount]
Value changes: HKLM\system\currentcontrolset\services\umbus\enum[count]
Value changes: HKLM\system\currentcontrolset\services\umbus\enum[nextinstance]
Value changes: HKLM\system\currentcontrolset\services\nativewifip\enum[count]
Value changes: HKLM\system\currentcontrolset\services\nativewifip\enum[nextinstance]
Value changes: HKLM\system\currentcontrolset\services\ndisuio\enum[count]
Value changes: HKLM\system\currentcontrolset\services\ndisuio\enum[nextinstance]
Value changes: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[status]