Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5, Task ID: 14

Task ID:	14
Risk Level:	7
Date Processed:	2016-04-07 08:21:31 (UTC)
Processing Time:	61.18 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
7 Injects thread into Windows process
2 Resolves local hostname
6 PE: File has TLS callbacks
3 Writes to a log file [Info]
4 Terminates process under Windows subfolder
4 Reads process memory
4 Connects to local IP
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: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
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]
Creates process: C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe]
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: EventLog [C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted]
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: PlugPlay [C:\Windows\system32\svchost.exe -k DcomLaunch]
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]
Reads from process: PID:2356 C:\Windows\SysWOW64\calc.exe
Terminates process: C:\Windows\System32\alg.exe
Terminates process: C:\Windows\System32\UIODetect.exe
Terminates process: C:\Windows\System32\VSSVC.exe
Terminates process: C:\Windows\System32\svchost.exe
Terminates process: C:\Windows\Temp\ToggleService32.exe
Terminates process: C:\Windows\System32\conhost.exe
Creates remote thread: System
Creates remote thread: C:\Windows\System32\svchost.exe
Creates remote thread: C:\Windows\explorer.exe
Creates remote thread: C:\Windows\System32\services.exe
Creates remote thread: C:\Windows\System32\sppsvc.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\MSDTC_STATS_EVENT
Creates mutex: \BaseNamedObjects\{00358dad-0e96-4bd1-837d-96e6cdd42d3b}_S-1-5-19
Creates mutex: \BaseNamedObjects\WIATRACE_MUTEX
Creates mutex: \BaseNamedObjects\d3b1bbc7-c020-4056-9ded-7c6f40b5a2fc
Creates mutex: \BaseNamedObjects\{11517B7C-E79D-4e20-961B-75A811715ADD}
Creates event: \BaseNamedObjects\RouterPreInitEvent
Creates event: \BaseNamedObjects\AudioSrv_CanAcceptMMCClient
Creates event: \BaseNamedObjects\WerSvcSystemPermissionsEvent
Creates event: \BaseNamedObjects\WiaServiceStarted
Creates event: \BaseNamedObjects\99b25af4-39cf-4c83-ad07-3c133e6d3135
Creates event: \Sessions\1\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY
Creates event: \Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61afb5}

File System Events

Creates: C:\Windows\SysWOW64\output.txt
Creates: C:\Windows\System32\MsDtc\Trace\dtctrace.log
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Creates: C:\ProgramData\Microsoft
Creates: C:\ProgramData\Microsoft\Crypto
Creates: C:\ProgramData\Microsoft\Crypto\RSA
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\31df4714b46f5e5ff8248d0fafa3b957_de228479-9e18-473a-b3d7-31d4d2573dc2
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
Creates: C:\Windows\ServiceProfiles\LocalService
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows
Creates: C:\Windows\SoftwareDistribution
Creates: C:\Windows\System32\spp\store\data.dat.tmp
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC\statecache.lock
Opens: C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\System32\conhost.exe
Opens: C:\Windows\System32\combase.dll
Opens: C:\Windows\System32\en-US\conhost.exe.mui
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\Windows\System32\en-US\user32.dll.mui
Opens: C:\Windows\system32\uxtheme.dll.Config
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\bcryptprimitives.dll
Opens: C:\Windows\System32\SHCore.dll
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\ToggleService32.exe
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\output.txt
Opens: C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\clbcatq.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\en-US\alg.exe.mui
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.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\msdtclog.dll
Opens: C:\Windows\System32\mtxclu.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\clusapi.dll
Opens: C:\Windows\System32\bcrypt.dll
Opens: C:\Windows\System32\xolehlp.dll
Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\Windows\System32\ktmw32.dll
Opens: C:\Windows\System32\resutils.dll
Opens: C:\Windows\System32\winmmbase.dll
Opens: C:\Windows\System32\cryptdll.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\MsDtc\Trace
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\Windows\DtcInstall.log
Opens: C:\Windows\System32\ntmarta.dll
Opens: C:\Windows\System32\MsDtc
Opens: C:\Windows\System32\MsDtc\MSDTC.LOG
Opens: C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
Opens: C:\Windows\System32\FirewallAPI.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
AppXDeploymentServer%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
NetworkProfile%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
StoreMgr%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
DeviceSetupManager%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
UserPnp%4DeviceInstall.evtx
Opens: C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
Opens: C:\Windows\System32\wtsapi32.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\winsta.dll
Opens: C:\Windows\System32\en-US\uiOdetect.exe.mui
Opens: C:\Windows\System32\adtschema.dll
Opens: C:\Windows\System32\services.exe
Opens: C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
Opens: C:
Opens: C:\$Extend
Opens: C:\ProgramData
Opens: C:\ProgramData\Microsoft
Opens: C:\ProgramData\Microsoft\Crypto
Opens: C:\ProgramData\Microsoft\Crypto\RSA
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\ServiceProfiles
Opens: C:\Windows\ServiceProfiles\LocalService
Opens: C:\Windows\ServiceProfiles\LocalService\AppData
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
Opens: C:\Windows\System32\en-US
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\svchost.exe
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\pnrpsvc.dll
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\gpapi.dll
Opens: C:\Windows\System32\powrprof.dll
Opens: C:\Windows\System32\profapi.dll

Opens: C:\Windows\System32\crypt32.dll
Opens: C:\Windows\System32\msasn1.dll
Opens:
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\358129098041A0483A25B784E8E10913_DE228479-9E18-
473A-B3D7-31D4D2573DC2
Opens: C:\Windows\System32\en-US\crypt32.dll.mui
Opens: C:\Windows\System32\dpapi.dll
Opens: C:\Windows\System32\ncrypt.dll
Opens: C:\Windows\System32\ntasn1.dll
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\System32\wuaueng.dll
Opens: C:\Windows\System32\en-US\wuaueng.dll.mui
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Opens: C:\Windows\System32\advapi32.dll
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\nsi.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\gdi32.dll
Opens: C:\Windows\System32\en-US\svchost.exe.mui
Opens: C:\Windows\System32\oleaut32.dll
Opens: C:\Windows\System32\ssdpapi.dll
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\5fe46d6f4fbbaedee4917a93b3902d78_de228479-9e18-
473a-b3d7-31d4d2573dc2
Opens: C:\Windows\System32\p2psvc.dll
Opens: C:\Windows\System32\P2PGraph.dll
Opens: C:\Windows\System32\esent.dll
Opens: C:\Windows\System32\en-US\p2psvc.dll.mui
Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\secur32.dll
Opens: C:\Windows\System32\slc.dll
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\d924c2fbb1b73c639740e02ee2ab504b_de228479-9e18-
473a-b3d7-31d4d2573dc2
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9C99BD1474CEB9C1AB13129747684184429ED3A1
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\4601d02f1df7da88667245cbda62ad09_de228479-9e18-
473a-b3d7-31d4d2573dc2
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\31df4714b46f5e5ff8248d0fafa3b957_de228479-9e18-
473a-b3d7-31d4d2573dc2
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\907a2f9ea01e84ee4723362858705197.sst
Opens: C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
Opens: C:\Windows\System32\spoolsv.exe
Opens: C:\Windows\System32\en-US\spoolsv.exe.mui
Opens: C:\Windows\System32\drivers\etc\lmhosts
Opens: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Opens: C:\Windows\System32\VSSVC.exe
Opens: C:\Windows\System32\vssapi.dll
Opens: C:\Windows\System32\vsstrace.dll
Opens: C:\Windows\System32\virtdisk.dll
Opens: C:\Windows\System32\dsrole.dll
Opens: C:\Windows\System32\fltLib.dll
Opens: C:\Windows\System32\en-US\VSSVC.exe.mui
Opens: C:\Windows\System32\vss_ps.dll
Opens: C:\Windows\System32\en-US\vsstrace.dll.mui
Opens: C:\Windows\System32\samcli.dll
Opens: C:\Windows\System32\netutils.dll
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\System32\sxs.dll
Opens: C:\Windows\System32\eventcls.dll
Opens: C:\Windows\System32\stdole2.tlb
Opens: C:\Windows\System32\msxml3.dll
Opens: C:\Windows\System32\shlwapi.dll
Opens: C:\Windows\System32\en-US\KernelBase.dll.mui
Opens: C:\Windows\System32\msxml3r.dll
Opens: C:\Windows\System32\setupapi.dll
Opens: C:\Windows\System32\cfgmgr32.dll
Opens: C:\Windows\System32\devobj.dll
Opens: C:\Windows\System32\en-US\setupapi.dll.mui
Opens: C:\Windows\System32\wintrust.dll

Opens: C:\Windows\System32\audiosrv.dll
Opens: C:\Windows\System32\hid.dll
Opens: C:\Windows\System32\avrt.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\debug
Opens: C:\Windows\debug\WIA
Opens: C:\Windows\System32\wiaservc.dll
Opens: C:\Windows\System32\wiatrace.dll
Opens: C:\Windows\System32\msv1_0.dll
Opens: C:\Windows\System32\sti.dll
Opens: C:\Windows\debug\WIA\wiatrace.log
Opens: C:\Windows\System32\Drivers\nwifi.sys
Opens: C:\Windows\apppatch\drvmain.sdb
Opens: C:\Windows\System32\Drivers\ndisuio.sys
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Virtualization-Client-Interop-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minio~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-shell~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-COM-MSMQ-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-vm~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
vm~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CommonFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-shell~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-HandwritingRecognizer-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-Base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Media-Streaming-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-

admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
NgenAssemblyExclusionClient~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpNamespace~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
PipeActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Personalization-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat

```
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalWMCEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Redhawk-v1.0-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDPProtocol-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDPProtocol-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
LanguagePack~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXLOB-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-OCUR-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Professional-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
sdktools~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sql~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
sql~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinSATMediaFiles-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\nt5.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntexe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntpe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntph.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem0.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-AM-Default-Definitions-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-legacy-whql.cat
Opens: C:\Windows\System32\kerberos.dll
Opens: C:\Windows\System32\wlanapi.dll
Opens: C:\Windows\System32\wlanhlp.dll
Opens: C:\Windows\System32\SubscriptionMgr.dll
Opens: C:\Windows\System32\wevtapi.dll
Opens: C:\Windows\System32\netcfgx.dll
Opens: C:\Windows\Inf
Opens: C:\Windows\Inf\netcfgx.0.etl
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Opens: C:\Windows\System32\dpapisrv.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
Opens: C:\Windows\System32\wlansvc.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx
Opens: C:\
Opens: C:\Windows\Temp
Opens: C:\Windows\Temp\ToggleService32.exe\
Opens: C:\Windows\System32\dps.dll

Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Opens: C:\Windows\System32\diagperf.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Opens: C:\Windows\System32\catroot2
Opens: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
Opens: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Opens: C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb\
Opens: C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
Opens: C:\Windows\system32\CatRoot2
Opens: C:\Windows\system32
Opens: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Opens: C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb\
Opens: C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\catroot2\edb.chk
Opens: C:\Windows\System32\catroot2\edb.log
Opens: C:\Windows\system32\CatRoot2\res1.log
Opens: C:\Windows\system32\CatRoot2\res2.log
Opens: C:\Windows\System32\catroot
Opens: C:\Windows\System32\sppsvc.exe
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
Opens: C:\Windows\Branding
Opens: C:\Windows\Branding\Basebrd
Opens: C:\Windows\System32\en-US\sppsvc.exe.mui
Opens: C:\Windows\System32\sppobjs.dll
Opens: C:\Windows\Branding\Basebrd\basebrd.dll
Opens: C:\Windows\System32\wwapi.dll
Opens: C:\Windows\System32\wscsvc.dll
Opens: C:\Windows\System32\dbghelp.dll
Opens: C:\Windows\System32\wbem\wbemprox.dll
Opens: C:\Windows\System32\wbemcomn.dll
Opens: C:\Windows\System32\wbem\wbemsvc.dll
Opens: C:\Windows\System32\wbem\fastprox.dll
Opens: C:\Windows\System32\winhttp.dll
Opens: C:\Windows\System32\wuapi.dll
Opens: C:\Windows\System32\cabinet.dll
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\WindowsUpdate.log
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\WindowsUpdate.log\
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local
Opens: C:\Windows\System32\wups.dll
Opens: C:\Windows\System32\userenv.dll
Opens: C:\Windows\System32\wkscli.dll
Opens: C:\Windows\System32\ci.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
Opens: C:\Windows\System32\spp\store\data.dat
Opens: C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifest-signed.xrm-ms
Opens: C:\Windows\System32\sppwinob.dll
Opens: C:\Windows\System32\netapi32.dll

Opens: C:\Windows\System32\srvcli.dll
Opens: C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-manifest-signed.xrm-ms
Opens: C:\Windows\System32\spp\store\cache\cache.dat
Opens: C:\Windows\System32\spp\store\tokens.dat
Opens: C:\Windows\System32\spp\store\data.dat.tmp
Opens: C:\Windows\System32\spp\store
Opens: C:\Windows\System32\spp\store\data.dat.bak
Opens: C:\Windows\System32\msxml6.dll
Opens: C:\Windows\System32\msxml6r.dll
Opens: C:\Windows\System32\taskschd.dll
Opens: C:\Windows\System32\wscinterop.dll
Opens: C:\Windows\System32\wscapi.dll
Opens: C:\Windows\System32\wscui.cpl
Opens: C:\Windows\System32\wscinterop.dll.123.Manifest
Opens: C:\Windows\System32\en-US\wscui.cpl.mui
Opens: C:\Windows\System32\werconcpl.dll
Opens: C:\Windows\System32\wer.dll
Opens: C:\Windows\System32\framedynos.dll
Opens: C:\Windows\System32\wercplsupport.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive
Opens: C:\ProgramData\Microsoft\Windows\WER\ReportArchive
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
Opens: C:\Windows\System32\hcproviders.dll
Opens: C:\Windows\System32\en-US\hcproviders.dll.mui
Opens: C:\Windows\System32\en-US\ActionCenter.dll.mui
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkAccessProtection%4WHC.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-Core%4WHC.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx
Opens: C:\Windows\System32\Actioncenter.dll.3.Manifest
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:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Writes to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\31df4714b46f5e5ff8248d0fafa3b957_de228479-9e18-473a-b3d7-31d4d2573dc2
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Writes to: C:\Windows\Inf\netcfgx.0.etl
Writes to: C:\Windows\System32\catroot2\edb.log
Writes to: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Writes to: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Writes to: C:\Windows\System32\spp\store\data.dat.tmp
Reads from: C:\Windows\SysWOW64\output.txt
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4DeviceInstall.evtx
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Reads from: C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
Reads from: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf

Reads from:	C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Reads from:	C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
Reads from:	C:\Windows\Inf\netcfgx.0.etl
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx
Reads from:	C:\Windows\Temp\ToggleService32.exe
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Reads from:	C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Reads from:	C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Reads from:	C:\Windows\System32\catroot2\edb.log
Reads from:	C:\Windows\System32\catroot2\edb.chk
Reads from:	C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
Reads from:	C:\Windows\System32\spp\store\data.dat
Reads from:	C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifest-signed.xrm-ms
Reads from:	C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-manifest-signed.xrm-ms
Reads from:	C:\Windows\System32\spp\store\cache\cache.dat
Reads from:	C:\Windows\System32\spp\store\tokens.dat
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkAccessProtection%4WHC.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-Core%4WHC.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx
Deletes:	C:\Windows\System32\spp\store\data.dat.tmp

Network Events

DNS query:	WPAD
Connects to:	10.74.12.255:138
Connects to:	10.74.12.255:137
Sends data to:	10.74.12.255:138
Sends data to:	10.74.12.255:137
Receives data from:	10.74.12.100:138
Receives data from:	10.74.12.100:137

Windows Registry Events

Creates key:	HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%12/8
Creates key:	HKCU\software\classes\local settings\muicache\13\52c64b7e
Creates key:	HKCU\software\classes\local settings\muicache
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\parameters
Creates key:	HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
Creates key:	HKLM\system\currentcontrolset\services\nativewifip
Creates key:	HKLM\system\currentcontrolset\services\ndisuio
Creates key:	HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache
Creates key:	HKLM\software\microsoft\windows

nt\currentversion\networklist\nla\cache\intranet
Creates key: HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet\
Creates key: HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\store
Creates key:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Creates key: HKLM\system\wpa
Creates key: HKLM\software\microsoft\security center\svc\vol
Creates key: HKLM\software\microsoft\security center
Creates key: HKLM\software\microsoft\security center\svc
Creates key: HKLM\software\microsoft\wbem\cimom
Creates key: HKLM\software
Creates key: HKLM\software\microsoft
Creates key: HKLM\software\microsoft\wbem
Creates key: HKLM\system\currentcontrolset\services\sharedaccess\epoch
Creates key: HKLM\software\microsoft\security center\monitoring
Creates key: HKLM\software\microsoft\windows\currentversion\policies\system
Creates key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100
Creates key: HKCU\software\microsoft\windows\windows error reporting
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0
Creates key: HKCU\software\microsoft\windows\currentversion\startupnotify
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{134ea407-755d-4a93-b8a6-f290cd155023}.check.8001
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
Creates key: HKCU\software\microsoft\windows\currentversion\action
center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100
Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]

Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]
Deletes value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserverlist]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpsubnetmaskopt]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdefaultgateway]
Deletes value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]
Deletes value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnetbiosoptions]
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\conhost.exe
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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\cmf\config
Opens key: HKLM\
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\windows nt\currentversion\console\truetypefont
Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
Opens key: HKCU\console
Opens key: HKCU\console\
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKCU\console\%systemroot%_temp_toggleservice32.exe
Opens key: HKCU\console\%systemroot%\temp\toggleservice32.exe
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
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\system\currentcontrolset\control\nls\codepage\eudccoderange
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
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\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
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\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\microsoft\rpc
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windowsruntime\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
Opens key: HKCR\activatableclasses\clsid
Opens key: HKCR\activatableclasses\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
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}\inprocserver32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\mui\settings
Opens key: HKCR\appid\alg.exe
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
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\software\microsoft\windowsruntime\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\activatableclasses\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\wow6432node\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCU\software\classes\activatableclasses\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\activatableclasses\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\wow6432node\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\activatableclasses\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\wow6432node\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\activatableclasses\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\wow6432node\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\activatableclasses\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\wow6432node\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\activatableclasses\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\wow6432node\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\activatableclasses\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\wow6432node\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKCR\activatableclasses\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
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\windows nt\currentversion\tracing\msdtc\misc
Opens key: HKLM\software\microsoft\msdtc
Opens key: HKCR\cid.local
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid
Opens key: HKCR\svcid.local
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log

Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\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\15546232-d044-45d4-88a8-0b84583f2fe1\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\4452c425-ad2f-4cde-b895-734b166ac4ac
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\description
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint
Opens key: HKCU\control panel\international
Opens key: HKLM\software\microsoft\rpc\securityservice
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\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties\dac
Opens key: HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc
Opens key: HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\activatableclasses\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
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}\inprocserver32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
Opens key: HKLM\software\policies\microsoft\windows nt\reliability
Opens key: HKLM\hardware\description\system\centralprocessor\0
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-appxdeploymentserver/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-networkprofile/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-kernel-storemgr/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-devicesetupmanager/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-userpnp/deviceinstall
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall
Opens key: HKU\.default\software\policies\microsoft\windows\safer\codeidentifiers
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: HKLM\software\microsoft\windows\currentversion\winevt
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences\0
Opens key: HKLM\system\currentcontrolset\services\eventlog\system\service control manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\localservicepeernet
Opens key: HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile
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\diagnostics
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\00000014
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\tcpip\parameters\winsock
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\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-25b8d56dd1d8}

Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
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: HKU\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
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\microsoft rsa schannel cryptographic provider
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
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\1.3.6.1.4.1.311.47.1.1!7
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKCU\software\classes\local settings\muicache\13\52c64b7e
Opens key: HKCU\software\classes\local settings\muicache
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\cryptdllfindoidinfo\1.3.6.1.4.1.311.76.6.1!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 nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe
Opens key: HKLM\system\currentcontrolset\control\print
Opens key: HKCR\clsid
Opens key: HKLM\software\policies\microsoft\windows nt\printers
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
Opens key: HKLM\system\currentcontrolset\services\lmhosts
Opens key: HKLM\system\currentcontrolset\services\lmhosts\parameters
Opens key: HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
Opens key: HKCR\appid\vssvc.exe
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
Opens key: HKCR\activatableclasses\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
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}\inprocserver32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
Opens key: HKCR\activatableclasses\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
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}\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: HKLM\software\microsoft\windowsruntime\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
Opens key: HKCR\activatableclasses\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
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}\inprocserver32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\activatableclasses\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
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}\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: HKLM\software\microsoft\windowsruntime\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\activatableclasses\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
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}\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: HKLM\software\microsoft\windowsruntime\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
Opens key: HKCR\activatableclasses\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
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}\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: HKLM\system\currentcontrolset\services\eventlog\application\vss
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKLM\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\render\
Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\audiosrv\parameters
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-a3cc-00a0c9223196}
Opens key: HKLM\software\microsoft\windows\currentversion\audio
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
Opens key: HKU\.default\control panel\international
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: HKLM\software\microsoft\windowsruntime\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKCR\activatableclasses\clsid\{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: HKLM\system\currentcontrolset\control\stillimage\fakedevices
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
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: HKLM\system\currentcontrolset\control\deviceclasses\{6bdd1fc6-810f-11d0-bec7-08002be2092f}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
Opens key: HKCR\activatableclasses\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
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}\inprocserver32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKCR\activatableclasses\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
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\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\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}
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\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-

6c15f82b5905}
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\parameters
Opens key: HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
Opens key: HKLM\system\currentcontrolset\services\ndisuio
Opens key: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&1&18
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000
Opens key: HKLM\system\currentcontrolset\services\nnetsecl\parameters
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage
Opens key: HKLM\system\currentcontrolset\services\wlansvc
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004
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}\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
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\linkage
Opens key: HKLM\system\currentcontrolset\services\wlansvc\linkage
Opens key: HKLM\system\currentcontrolset\services\wlansvc\parameters
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\system\currentcontrolset\enum\root*isatap\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\linkage
Opens key: HKLM\system\currentcontrolset\enum\root*teredo\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}
Opens key: HKLM\software\microsoft\wcmsvc
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\properties
Opens key: HKLM\software\microsoft\wcmsvc\subscriptionmanager
Opens key: HKLM\system\currentcontrolset\control\cryptography\providers
Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
Opens key: HKCR\activatableclasses\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\treatas
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandler32
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandler

Opens key: HKLM\system\currentcontrolset\control\network
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wcmsvc/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wcmsvc/diagnostic
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-crypto-dpapi/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-crypto-dpapi/backupkeysvc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-crypto-dpapi/debug
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wlan-autoconfig/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wlan-autoconfig/diagnostic
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKLM\system\currentcontrolset\control\diagnostics\performance
Opens key: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnosis-dps/debug
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnosis-dps/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnosis-dps/analytic
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnostics-performance/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-

diagnostics-performance/diagnostic
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnostics-performance/diagnostic/loopback
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key: HKLM\system\currentcontrolset\services\{b5105d63-74c6-4dc1-87b7-55779daa70e9}\parameters\tcpip
Opens key: HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Opens key: HKLM\system\currentcontrolset\services\netbt\adapters\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKLM\system\currentcontrolset\services\dnscache
Opens key: HKLM\system\currentcontrolset\services\dnscache\startoverride
Opens key: HKLM\software\microsoft\ctf\knownclasses
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\startoverride
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper
Opens key: HKLM\system\currentcontrolset\services\rpcss
Opens key: HKLM\system\currentcontrolset\services\sppsvc
Opens key: HKU\s-1-5-20
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20
Opens key: HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKU\s-1-5-20\environment
Opens key: HKU\s-1-5-20\volatile environment
Opens key: HKU\s-1-5-20\volatile environment\0
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sppsvc.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\quota system\s-1-5-20
Opens key: HKCR\appid\sppsvc.exe
Opens key: HKLM\system\currentcontrolset\services\eventlog\application\software protection platform service
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
Opens key: HKLM\system\currentcontrolset\services\wsearch
Opens key: HKLM\system\currentcontrolset\services\http
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key: HKLM\system\currentcontrolset\services\winmgmt
Opens key: HKLM\system\currentcontrolset\services\wscsvc
Opens key: HKLM\system\currentcontrolset\services\wscsvc\parameters
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18
Opens key: HKLM\software\microsoft\security center\svc\vol
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19
Opens key: HKLM\software\microsoft\security center\svc
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\activatableclasses\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\elevation
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\elevation
Opens key: HKCR\unmarshalers\system\{00000339-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\activatableclasses\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler
Opens key: HKLM\software\microsoft\wbem\cimom
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
Opens key: HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
Opens key: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
Opens key: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas
Opens key: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver32
Opens key: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler32
Opens key: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler
Opens key: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
Opens key: HKCR\activatableclasses\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
Opens key: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
Opens key: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\treatas
Opens key: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32
Opens key: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprochandler32
Opens key: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprochandler
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\forward
Opens key: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\typelib
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\activatableclasses\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}
Opens key: HKCR\activatableclasses\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}
Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}
Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\treatas
Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22
Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprochandler32
Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\compression
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\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\software\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\misc
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\report
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\setup
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\service
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\agent
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\au
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\auclnt
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cltui
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cpl
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuapp
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuweb
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\dtastor
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cdm
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\pt
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\driver
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\comapi
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\parser
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\handler
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\eehndlr
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\dnldmgr
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cmpress
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\shutdwn
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuredir
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\offlsnc
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\inv
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\arp
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\trace
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\tracetestmain
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\tracetestthreads
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\perf,
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\ws
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\ep
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wutask
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\mowu
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\rebootnotify
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdatesysprepinprogress
Opens key: HKLM\software\policies\microsoft\windows\windowsupdate
Opens key: HKLM\software\policies\microsoft\windows\windowsupdate\au
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update
Opens key: HKCU\software\microsoft\windows\currentversion\policies\windowsupdate
Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update\rebootrequired
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3
Opens key:
HKLM\software\microsoft\windows\currentversion\networkservicetriggers\triggers\bc90d167-9470-4139-a9ba-be0bbbf5b74d\2fb92682-6599-42dc-ae13-bd2ca89bd11c
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
Opens key:
HKLM\system\currentcontrolset\services\eventlog\application\securitycenter
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5

Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-codeintegrity/operational
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-codeintegrity/verbose
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose
Opens key: HKCU\software\microsoft\windows nt\currentversion\softwareprotectionplatform\persistedtsrearmed
Opens key: HKCU\software\microsoft\windows nt\currentversion\softwareprotectionplatform\persistedsystemstate
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-1200ef9b32a
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key: HKCU\software\microsoft\windows nt\currentversion\softwareprotectionplatform

Opens key: HKLM\software\microsoft\windows nt\currentversion\
Opens key: HKLM\system\setup\status
Opens key: HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\reboot.sl_brt_commit
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0
Opens key:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0
Opens key: HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09
Opens key: HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0
Opens key:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_____1.0.7.3_\5&34baf594&0&0.0.0
Opens key: HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34\
Opens key: HKLM\system\wpa\
Opens key: HKLM\system\wpa\478c035f-04bc-48c7-b324-2462d786dad7-5p-9\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8\
Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9\
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}
Opens key: HKCR\activatableclasses\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
Opens key: HKLM\software\microsoft\msxml60
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}
Opens key: HKCR\activatableclasses\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}
Opens key: HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32
Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\parameters
Opens key: HKLM\software\microsoft\windows\currentversion\action

center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCR\activatableclasses\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
Opens key: HKLM\software\microsoft\security center
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key: HKLM\software\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKLM\system\currentcontrolset\services\wscsvc\startoverride
Opens key: HKLM\software\policies\microsoft\windows defender
Opens key: HKLM\software\policies\microsoft\windows defender\real-time protection
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCR\activatableclasses\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
Opens key: HKLM\software\policies\microsoft\windows\windows error reporting
Opens key: HKCU\software\policies\microsoft\windows\windows error reporting
Opens key: HKCU\software\microsoft\windows\windows error reporting
Opens key: HKLM\software\microsoft\windows\windows error reporting\syspreplock
Opens key: HKCU\software\microsoft\windows\windows error reporting\erc
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-

0040963251e5}\inprochandler
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
Opens key: HKCR\activatableclasses\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas
Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas
Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32
Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32
Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32
Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler
Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key: HKCR\activatableclasses\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas
Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas
Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32
Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32
Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32
Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32
Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler
Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\startupnotify
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCR\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-

40cd513679d5}\inprochandler
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-windowsbackup/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-networkaccessprotection/whc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-windows defender/whc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnosis-scheduled/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-taskscheduler/maintenance
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-homegroup control panel/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-security-spp-ux-notifications/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{b447b4db-7780-11e0-ada3-18a90531a85a}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-filehistory-core/whc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-ntfs/whc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-shell-connectedaccountstate/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{96f4a050-7e31-453c-88be-9634f4e02139}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-userpnp/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-storagespaces-managementagent/whc
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc
Opens key: HKLM\software\microsoft\windows\currentversion\action center
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[conhost]
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\ole[aggressivemtatesting]
Queries value: HKCU\console[screencolors]
Queries value: HKCU\console[popupcolors]
Queries value: HKCU\console[insertmode]
Queries value: HKCU\console[quickedit]
Queries value: HKCU\console[codepage]
Queries value: HKCU\console[screenbuffersize]
Queries value: HKCU\console[windowsize]
Queries value: HKCU\console[windowposition]
Queries value: HKCU\console[fontsize]
Queries value: HKCU\console[fontfamily]
Queries value: HKCU\console[fontweight]
Queries value: HKCU\console[facename]
Queries value: HKCU\console[cursorsize]
Queries value: HKCU\console[historybuffersize]
Queries value: HKCU\console[numberofhistorybuffers]
Queries value: HKCU\console[historynodup]
Queries value: HKCU\console[colortable00]
Queries value: HKCU\console[colortable01]
Queries value: HKCU\console[colortable02]
Queries value: HKCU\console[colortable03]
Queries value: HKCU\console[colortable04]
Queries value: HKCU\console[colortable05]
Queries value: HKCU\console[colortable06]
Queries value: HKCU\console[colortable07]
Queries value: HKCU\console[colortable08]
Queries value: HKCU\console[colortable09]
Queries value: HKCU\console[colortable10]
Queries value: HKCU\console[colortable11]
Queries value: HKCU\console[colortable12]
Queries value: HKCU\console[colortable13]
Queries value: HKCU\console[colortable14]
Queries value: HKCU\console[colortable15]
Queries value: HKCU\console[loadconime]
Queries value: HKCU\console[extendededitkey]
Queries value: HKCU\console[extendededitkeycustom]
Queries value: HKCU\console[worddelimiters]
Queries value: HKCU\console[trimleadingzeros]
Queries value: HKCU\console[enablecolorselection]
Queries value: HKCU\console[scrollscale]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
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: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[toggleservice32.exe]
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\rpc[idletimerwindow]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]
Queries value: HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
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\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\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\sources[trace_wmi]
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\windows nt\currentversion\tracing\msdtc\misc[disabletracing]
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\msdtc[disableterminationonheapcorruption]
Queries value: HKLM\software\microsoft\msdtc[sysprepinprogress]
Queries value: HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid[]
Queries value: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log\size[]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalibpath]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllibpath]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracleocilibpath]
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\15546232-d044-45d4-88a8-0b84583f2fe1\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\4452c425-ad2f-4cde-b895-734b166ac4ac\description[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid[]
Queries value: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint[]
Queries value: HKCU\control panel\international[scurrencyoverride]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\microsoft\msdtc[notracking]
Queries value: HKLM\software\microsoft\rpc\securityservice[9]
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\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid[]
Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid[]
Queries value: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\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\software\microsoft\msdtc[logwarnenabled]
Queries value: HKLM\software\microsoft\msdtc[suppressduplicateduration]
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\currentversion\reliability[timestampinterval]
Queries value: HKLM\hardware\description\system\centralprocessor\0[~mhz]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-appxdeploymentserver/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[maxbuffers]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[autobackuplogfiles]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernel-storemgr/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-devicesetupmanager/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[filecounter]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/deviceinstall[channelaccess]
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\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[categorymessagefile]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences[count]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences\0[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences\0[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences\0[id]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system\service control manager[providerguid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[localservicepeernet]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile[svchost]
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\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
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\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
Queries value: HKLM\software\microsoft\sqmclient[machineid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[seedserver]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastpublish]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastsearch]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[searchonly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[mincpalifetime]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
19[profileimagepath]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
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\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
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\policies\microsoft\cryptography[forcekeyprotection]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]
Queries value:

HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
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\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.76.6.1!7[name]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[disableheaplookaside]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[frontendheapdebugoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[shutdownflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[unloadeventtracedepth]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[tracingflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[minimumstackcommitinbytes]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[breakoninitializeprocessfailure]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[keepactivationcontextsalive]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[trackactivationcontextreleases]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[maxdeadactivationcontexts]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[globalflag]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[cwdillegalindllsearch]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[debugprocessheaponly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[searchpathmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[spoolsv]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d2e1bab2-eb9b-4ba7-9123-19c01ddc4f78]
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\wmi\security[b1ad9b49-051a-4896-ae24-ebc9b8676e76]
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\software\microsoft\sqmclient\windows[studyid]
Queries value: HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
Queries value: HKLM\system\currentcontrolset\control\print[callexitprocessonshutdown]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\parameters[enableusermode]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e14dcdd9-d1ec-4dc3-8395-a606df8ef115]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[4d20df22-e177-4514-a369-f1759feedeb3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
Queries value: HKLM\software\microsoft\com3[finalizeractivitybypass]
Queries value: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
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}[]
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}[]
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: HKLM\system\currentcontrolset\services\eventlog\application\vss[providerguid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[displayversion]
Queries value: HKCU\control panel\desktop[paintdesktopversion]
Queries value: HKLM\system\currentcontrolset\services\audiosrv\parameters[servicedllunloadonstop]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
Queries value: HKLM\software\microsoft\windows\currentversion\audio[enablecapturemonitor]
Queries value: HKU\.default\control panel\international[scurrencyoverride]
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}[]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
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\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[name]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[desc]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[icon]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[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\{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\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[icon]

Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[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[pnpflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-99ea-fe66a8355df8]
Queries value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
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\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindonattach]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindondetach]
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\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&1&18[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010\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}\0007\linkage[upperbind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage[upperbind]
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\services\ndisuio[legacypause]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[ndisbootstart]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[wow64]
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}\0000\linkage[upperbind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[requiredprivileges]
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\services\wlansvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\enum\root*isatap\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root*teredo\0000[driver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d81-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-

0000-000000000000]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012\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}\0002\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d80-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\software\microsoft\wcmsvc[wlanminsignalstrength]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008[netcfginstanceid]
Queries value: HKLM\software\microsoft\wcmsvc[wlanweaksignalmeasureinterval]
Queries value: HKLM\software\microsoft\wcmsvc[wlangoodsignalmeasureinterval]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010[characteristics]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[082f46b6-01f6-4511-9044-d83675f46637]
Queries value: HKLM\software\microsoft\wcmsvc\subscriptionmanager[servertimeretryperiod]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011[characteristics]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012[characteristics]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}[]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b6c2b638-4f86-4095-9446-dfc044e0663a]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[41e8e8f3-7b6d-488e-b350-f696dd24afb6]
Queries value: HKLM\system\currentcontrolset\control\network[config]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[messagefilename]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[categorymessagefile]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[resourcefilename]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[parameterfilename]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[helplink]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[enabled]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-fa9117f3e6f2}[categorycount]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[type]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

wcmsvc/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

wcmsvc/diagnostic[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[channelaccess]
Queries value: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
Queries value: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[clocktype]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[filterid]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/debug[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[helplink]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[maxbuffers]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-autoconfig/diagnostic[channelaccess]
Queries value: HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\store[c:\windows\temp\toggleservice32.exe]
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\autologger\circular kernel context logger[stackcaching]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-

af71-3e63d056f174]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-

dps/debug[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-

dps/analytic[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/analytic[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-

performance/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-

performance/diagnostic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-

performance/diagnostic/loopback[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[channelaccess]
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[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[enableipautoconfigurationlimits]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[ipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[subnetmask]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[ipautoconfigurationaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[performrouterdiscovery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[defaultgateway]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[defaultgatewaymetric]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[solicitationaddressbcast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[usezerobroadcast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[typeofinterface]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}[mtu]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[interfacemetric]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[tcpackfrequency]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[tcpdelackticks]
Queries value:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dnscache[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache[start]
Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dnscache[tag]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dnscache[group]
Queries value: HKLM\system\currentcontrolset\services\dnscache[objectname]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[type]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[start]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[group]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpcss[objectname]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
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-1-5-20[profileimagepath]
Queries value: HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[environment]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[startprotected]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[sppsvc]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-a5f9-f2bdfea0f156]
Queries value: HKLM\system\currentcontrolset\services\eventlog\application\software protection platform service[providerguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[categorycount]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[inactivityshutdowndelay]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[keeprunningthresholdmins]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[tokenstore]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1[]

Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
Queries value: HKLM\system\currentcontrolset\services\wsearch[objectname]
Queries value: HKLM\system\currentcontrolset\services\http[objectname]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\winmgmt[objectname]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\wscsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\wscsvc\parameters[servicemain]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
809b-2a87b70881f8]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-
8539-9230a44081a5]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
Queries value: HKLM\software\microsoft\security center\svc[vistasp1]
Queries value: HKLM\software\microsoft\security center\svc[antivirusoverride]
Queries value: HKLM\software\microsoft\security center\svc[antispywareoverride]
Queries value: HKLM\software\microsoft\security center\svc[firewalloverride]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[serviceparameters]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[runas]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[activateatstorage]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[rotflags]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appidflags]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[launchpermission]
Queries value: HKLM\software\microsoft\ole[legacyauthenticationlevel]
Queries value: HKLM\software\microsoft\ole[legacyimpersonationlevel]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[authenticationlevel]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[remoteservername]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[srptrustlevel]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}[preferredserverbitness]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[loadusersettings]
Queries value: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
Queries value: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
Queries value: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
Queries value: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[processid]
Queries value: HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
Queries value: HKLM\software\microsoft\wbem\cimom[contextlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[objectlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[identifierlimit]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
Queries value: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
Queries value: HKCR\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver32[]
Queries value: HKCR\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]

Queries value: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\proxystubclsid32[]
Queries value: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}[]
Queries value: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32[]
Queries value: HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}[interfacehelperdisableall]
Queries value: HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}[interfacehelperuser]
Queries value: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}[]
Queries value: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32[]
Queries value: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32[threadingmodel]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22[]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsingname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
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\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25[]
Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[auoptions]
Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[autoinstallminorupdates]
Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[includerecommendedupdates]
Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[elevatenonadmins]
Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[configver]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3[]
Queries value: HKLM\software\microsoft\security center[cval]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30[]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\application\securitycenter[providerguid]

Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[consentpromptbehavioradmin]
Queries value:
HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8[]
Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[file]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-codeintegrity/verbose[channelaccess]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a[manifestfile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a[pluginfile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662[manifestfile]

Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662[pluginfile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[moduleid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[isservice]
Queries value: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[isservice]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[isservice]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[isservice]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[kmshostconfig]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[vlactivationinterval]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[vlrenewalinterval]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[actionlist]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[publisherpolicychangetime]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[cachestore]
Queries value: HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
Queries value: HKLM\system\setup\status[auditboot]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[hardwareid]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[compatibleids]
Queries value: HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_____1.0.7.3_\5&34baf594&0&0.0.0[hardwareid]
Queries value:

HKLM\system\currentcontrolset\enum\ide\diskhitachi_____1.0.7.3_\5&34baf594&0&0.0.0[compatibleids]
Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[hardwareid]
Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[compatibleids]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[licstatusarray]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[policyvaluesarray]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[hasooberun]
Queries value: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}[]
Queries value: HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32[]
Queries value: HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}[]
Queries value: HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[]
Queries value: HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[servicesessionid]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[logcontext]
Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[productpolicy]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\parameters[servicedllunloadonstop]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-
833b-323e85a1ce84]
Queries value: HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
Queries value: HKLM\software\policies\microsoft\internet
explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
Queries value: HKLM\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[type]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[start]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[group]
Queries value: HKLM\software\microsoft\security center[autoupdatedisablenotify]
Queries value: HKLM\software\microsoft\security center[internetsettingsdisablenotify]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104[checksetting]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[logging]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[a0ef609d-0a14-424c-
9270-3b2691a0a394]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-
86ba-948b70416220]
Queries value: HKLM\software\microsoft\windows\windows error reporting[disabled]
Queries value: HKCU\software\microsoft\windows\windows error reporting[disabled]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]

Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\windows error reporting[lastqueuepestertime]
Queries value: HKLM\software\microsoft\windows\windows error reporting[queuepesterinterval]
Queries value: HKCU\software\microsoft\windows\windows error reporting[queuepesterinterval]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
Queries value: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
Queries value: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]
Queries value: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[threadingmodel]
Queries value: HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[smartscreenenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
Queries value: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}[]
Queries value: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
Queries value: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\startupnotify[enablestartupappnotification]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[type]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[enabled]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[filemax]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[filecounter]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[buffersize]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[minbuffers]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[maxbuffers]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[latency]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[clocktype]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[sidtype]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[level]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[controlguid]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[maxsize]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

windowsbackup/actioncenter[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windowsbackup/actioncenter[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}[lastknownstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkaccessprotection/whc[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

networkaccessprotection/whc[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[type]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[enabled]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[filemax]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[filecounter]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[buffersize]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[minbuffers]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[maxbuffers]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[latency]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[clocktype]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[sidtype]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[level]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[controlguid]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[maxsize]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[maxsizeupper]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[retention]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[autobackuplogfiles]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[file]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[filterid]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[isolation]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[owningpublisher]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[type]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[enabled]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[filemax]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[filecounter]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[buffersize]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[minbuffers]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-scheduled/operational[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[maxsizeupper]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-taskscheduler/maintenance[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}[lastknownstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroupcontrol panel/operational[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{134ea407-755d-4a93-b8a6-f290cd155023}.check.8001[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action

center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}[lastknownstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100[checksetting]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[latency]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100[checksetting]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[file]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}[lastknownstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100[checksetting]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[filemax]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-userpnp/actioncenter[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}[lastknownstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[level]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespaces-managementagent/whc[channelaccess]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100[checksetting]
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\services\nativewifip[drivermajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[driverminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[ndisminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[drivermajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[driverminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpsubnetmaskopt]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdefaultgateway]
Sets/Creates value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34[]
Value changes: HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache\intranet[{b5105d63-74c6-4dc1-87b7-55779daa70e9}]
Value changes: HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\store[c:\windows\temp\toggleservice32.exe]
Value changes: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[status]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[hrzr_pgyfrffvba]
Value changes:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpinterfaceoptions]
Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[servicesessionid]
Value changes: HKLM\software\microsoft\security center[cval]
Value changes: HKLM\software\microsoft\security center\svc[antivirusoverride]
Value changes: HKLM\software\microsoft\security center\svc[antispywareoverride]
Value changes: HKLM\software\microsoft\security center\svc[firewalloverride]
Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[licstatusarray]
Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[actionlist]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action

center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
  Value changes: HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
  Value changes: HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
  Value changes: HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]