Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 758

Task ID:	758
Risk Level:	10
Date Processed:	2016-05-18 10:34:35 (UTC)
Processing Time:	63.15 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"
Sample ID:	3312
Type:	basic
Owner:	admin
Label:	859ba9477553ccad1bba34c555ab6a1b
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	199680 bytes
MD5:	859ba9477553ccad1bba34c555ab6a1b
SHA256:	339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1
Description:	None

Pattern Matching Results

7 Writes to memory of system processes
6 Modifies registry autorun entries
6 Writes to system32 folder
2 PE: Nonstandard section
3 HTTP connection - response code 200 (success)
7 Injects thread into Windows process
6 Changes Winsock providers
10 Creates malicious events: ZeroAccess [Rootkit]
4 Terminates process under Windows subfolder
4 Reads process memory
5 PE: Contains compressed section
5 Abnormal sleep detected
3 Long sleep detected
5 Installs service

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe ["C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"]
Creates process:	C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange]
Creates process:	C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"]
Reads from process:	PID:3052 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:340 C:\Windows\explorer.exe
Writes to process:	PID:444 C:\Windows\System32\services.exe
Writes to process:	PID:2780 C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Terminates process:	C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Creates remote thread:	C:\Windows\explorer.exe
Creates remote thread:	C:\Windows\System32\services.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\BaseNamedObjects\ConsoleEvent-0x0000000000000AEC

File System Events

Creates:	C:\$Recycle.Bin\
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\L
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates: C:\$Recycle.Bin\S-1-5-18
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\L
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates: C:GAC_MSIL
Creates: C:GAC
Creates: C:GAC_32
Creates: C:GAC_64
Creates: C:\Windows\assembly\GAC_64\Desktop.ini
Creates: C:\Windows\assembly\GAC_32\Desktop.ini
Creates: C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Creates: C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
Creates: C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
Opens: C:\Windows\Prefetch\859BA9477553CCAD1BBA34C555AB6-401FB0A4.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\atl.dll
Opens: C:\Windows\SysWOW64\atl.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\djusifdsjufkjldsdljkfh
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\Cabinet.dll
Opens: C:\Windows\SysWOW64\cabinet.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens: C:\windows\temp\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens: C:\Windows\MSWSOCK.dll
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens: C:\Windows\assembly
Opens: C:\Windows\assembly\GAC_32\Desktop.ini
Opens: C:\Windows\assembly\GAC_64\Desktop.ini
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Opens: C:\Windows\SysWOW64\cmd.exe
Opens: C:\Windows\Temp
Opens: C:\Windows\System32\rundll32.exe
Opens: C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
Opens: C:\Windows\System32
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\
Opens: C:\Windows\SysWOW64\ui\SwDRM.dll
Opens: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Opens: C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens: C:\Windows\SysWOW64\winbrand.dll
Opens: C:\Windows\SysWOW64\en-US\cmd.exe.mui
Opens: C:\Windows\System32\LogFiles\Scm\d22b06f4-3c25-4d82-b665-f21eb07c8662
Opens: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\en-US\rundll32.exe.mui
Opens: C:\Windows\System32\BFE.DLL
Opens: C:\Windows\system32\bfe.dll.manifest
Opens: C:\Windows\system32\bfe.dll.123.Manifest
Opens: C:\Windows\system32\bfe.dll.124.Manifest
Opens: C:\Windows\system32\bfe.dll.2.Manifest
Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\slc.dll
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
Opens: C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Opens: C:\Windows\System32\LogFiles\Scm\2f57269b-1e09-4e2d-ab1e-b0fdac7d279c
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
Opens: C:\Windows\SysWOW64\calc.exe
Opens: C:\Windows\System32\UIAnimation.dll
Opens: C:\Users\Admin\Desktop
Writes to: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@

Writes to:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Writes to:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Writes to:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Writes to:	C:\Windows\assembly\GAC_64\Desktop.ini
Writes to:	C:\Windows\assembly\GAC_32\Desktop.ini
Writes to:	C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Writes to:	C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
Writes to:	C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
Reads from:	C:\Windows\SysWOW64\cmd.exe
Reads from:	C:\Windows\System32\LogFiles\Scm\d22b06f4-3c25-4d82-b665-f21eb07c8662
Reads from:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Reads from:	C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Reads from:	C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
Reads from:	C:\Windows\System32\LogFiles\Scm\2f57269b-1e09-4e2d-ab1e-b0fdac7d279c
Deletes:	C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Network Events

DNS query:	promos.fling.com
DNS response:	promos.fling.com ⇒ 208.91.207.58
Connects to:	208.91.207.58:80
Connects to:	213.108.252.185:80
Sends data to:	8.8.8.8:53
Sends data to:	promos.fling.com:80 (208.91.207.58)
Sends data to:	213.108.252.185:80
Sends data to:	83.133.123.20:53
Sends data to:	66.169.64.252:16470
Sends data to:	70.245.30.44:16470
Sends data to:	24.166.74.57:16470
Sends data to:	84.238.123.251:16470
Sends data to:	98.200.159.59:16470
Sends data to:	24.166.102.61:16470
Sends data to:	207.253.171.66:16470
Sends data to:	76.90.0.73:16470
Sends data to:	99.250.124.73:16470
Sends data to:	90.129.15.104:16470
Sends data to:	207.98.234.114:16470
Sends data to:	75.177.68.122:16470
Sends data to:	209.20.29.125:16470
Sends data to:	98.203.59.126:16470
Sends data to:	98.223.143.132:16470
Sends data to:	68.44.66.138:16470
Sends data to:	67.183.232.147:16470
Sends data to:	81.233.194.148:16470
Sends data to:	90.237.150.151:16470
Sends data to:	76.17.49.27:16470
Sends data to:	75.71.170.178:16470
Sends data to:	94.191.193.25:16470
Sends data to:	64.244.39.17:16470
Sends data to:	190.172.245.16:16470
Sends data to:	70.66.158.194:16470
Sends data to:	180.215.28.200:16470
Sends data to:	62.143.199.5:16470
Sends data to:	68.35.93.217:16470
Sends data to:	24.7.243.232:16470
Sends data to:	76.84.200.232:16470
Sends data to:	113.211.25.228:16470
Sends data to:	108.162.165.226:16470
Sends data to:	65.26.156.226:16470
Sends data to:	184.58.36.223:16470
Sends data to:	202.147.221.2:16470
Sends data to:	83.254.124.221:16470
Sends data to:	121.73.119.3:16470
Sends data to:	206.174.8.235:16470
Sends data to:	173.179.2.4:16470
Sends data to:	81.233.3.4:16470
Sends data to:	176.198.31.4:16470
Sends data to:	89.239.230.213:16470
Sends data to:	24.252.143.4:16470
Sends data to:	189.106.146.212:16470
Sends data to:	24.223.187.210:16470
Sends data to:	24.60.167.210:16470
Sends data to:	70.80.21.5:16470
Sends data to:	96.22.40.5:16470
Sends data to:	68.224.54.5:16470
Sends data to:	113.35.220.208:16470
Sends data to:	107.9.219.208:16470
Sends data to:	68.59.113.5:16470
Sends data to:	87.50.25.235:16470
Sends data to:	62.75.219.6:16470
Sends data to:	122.132.159.11:16470
Sends data to:	76.109.133.206:16470

Receives data from: 0.0.0.0:0
Receives data from: promos.fling.com:80 (208.91.207.58)
Receives data from: 213.108.252.185:80

Windows Registry Events

Creates key: HKCU\software\classes\clsid
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32
Deletes value: HKLM\software\microsoft\windows\currentversion\run[windows defender]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
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\2f2e863f
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_entries
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0
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\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
Opens key: HKLM\software\microsoft\windows\currentversion\run
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: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
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\000000000008
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\000000000006
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\000000000004
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\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
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\000000000004
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\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base

cryptographic provider v1.0
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key: HKU\.default\environment
Opens key: HKU\.default\volatile environment
Opens key: HKU\.default\volatile environment\0
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
Opens key: HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\rundll32.exe
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc
Opens key: HKLM\system\currentcontrolset\services\alg
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\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bthserv
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64
Opens key: HKLM\system\currentcontrolset\services\comsysapp
Opens key: HKLM\system\currentcontrolset\services\cryptsvc
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch
Opens key: HKLM\system\currentcontrolset\services\defragsvc
Opens key: HKLM\system\currentcontrolset\services\dnscache
Opens key: HKLM\system\currentcontrolset\services\dot3svc
Opens key: HKLM\system\currentcontrolset\services\eaphost
Opens key: HKLM\system\currentcontrolset\services\efs
Opens key: HKLM\system\currentcontrolset\services\ehrecvr
Opens key: HKLM\system\currentcontrolset\services\ehsched
Opens key: HKLM\system\currentcontrolset\services\eventsystem
Opens key: HKLM\system\currentcontrolset\services\fax
Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdrespub
Opens key: HKLM\system\currentcontrolset\services\fontcache
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0
Opens key: HKLM\system\currentcontrolset\services\hidserv
Opens key: HKLM\system\currentcontrolset\services\hkmsvc
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider
Opens key: HKLM\system\currentcontrolset\services\idsvc
Opens key: HKLM\system\currentcontrolset\services\ivmservice
Opens key: HKLM\system\currentcontrolset\services\keyiso
Opens key: HKLM\system\currentcontrolset\services\ktmrm
Opens key: HKLM\system\currentcontrolset\services\lltdsvc
Opens key: HKLM\system\currentcontrolset\services\mcx2svc
Opens key: HKLM\system\currentcontrolset\services\msdtc
Opens key: HKLM\system\currentcontrolset\services\msiscsi
Opens key: HKLM\system\currentcontrolset\services\msiserver
Opens key: HKLM\system\currentcontrolset\services\napagent

Opens key: HKLM\system\currentcontrolset\services\netlogon
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing
Opens key: HKLM\system\currentcontrolset\services\ose
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc
Opens key: HKLM\system\currentcontrolset\services\p2psvc
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc
Opens key: HKLM\system\currentcontrolset\services\perfhost
Opens key: HKLM\system\currentcontrolset\services\pla
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc
Opens key: HKLM\system\currentcontrolset\services\policyagent
Opens key: HKLM\system\currentcontrolset\services\protectedstorage
Opens key: HKLM\system\currentcontrolset\services\rasauto
Opens key: HKLM\system\currentcontrolset\services\rasman
Opens key: HKLM\system\currentcontrolset\services\remoteaccess
Opens key: HKLM\system\currentcontrolset\services\remoteregistry
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper
Opens key: HKLM\system\currentcontrolset\services\rpclocator
Opens key: HKLM\system\currentcontrolset\services\samss
Opens key: HKLM\system\currentcontrolset\services\scardsvr
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc
Opens key: HKLM\system\currentcontrolset\services\sdrsvc
Opens key: HKLM\system\currentcontrolset\services\seclogon
Opens key: HKLM\system\currentcontrolset\services\sensrsvc
Opens key: HKLM\system\currentcontrolset\services\snmptrap
Opens key: HKLM\system\currentcontrolset\services\spooler
Opens key: HKLM\system\currentcontrolset\services\sppsvc
Opens key: HKLM\system\currentcontrolset\services\sppuinotify
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv
Opens key: HKLM\system\currentcontrolset\services\sstpsvc
Opens key: HKLM\system\currentcontrolset\services\stisvc
Opens key: HKLM\system\currentcontrolset\services\storsvc
Opens key: HKLM\system\currentcontrolset\services\swprv
Opens key: HKLM\system\currentcontrolset\services\sysmain
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice
Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\tbs
Opens key: HKLM\system\currentcontrolset\services\threadorder
Opens key: HKLM\system\currentcontrolset\services\tlntsvr
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller
Opens key: HKLM\system\currentcontrolset\services\ui0detect
Opens key: HKLM\system\currentcontrolset\services\upnphost
Opens key: HKLM\system\currentcontrolset\services\vaultsvc
Opens key: HKLM\system\currentcontrolset\services\vds
Opens key: HKLM\system\currentcontrolset\services\vss
Opens key: HKLM\system\currentcontrolset\services\wbengine
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice
Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\wecsvc
Opens key: HKLM\system\currentcontrolset\services\wercplsupport
Opens key: HKLM\system\currentcontrolset\services\wersvc
Opens key: HKLM\system\currentcontrolset\services\winrm
Opens key: HKLM\system\currentcontrolset\services\wlansvc
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key: HKLM\system\currentcontrolset\services\wpcsvc
Opens key: HKLM\system\currentcontrolset\services\wsearch
Opens key: HKLM\system\currentcontrolset\services\wuauserv
Opens key: HKLM\system\currentcontrolset\services\wudfsvc
Opens key: HKLM\system\currentcontrolset\services\wwansvc
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\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0

Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\certpropsvc
Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
Opens key:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\triggerinfo
Opens key:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cscservice
Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dhcp
Opens key: HKLM\system\currentcontrolset\services\dhcp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dps
Opens key: HKLM\system\currentcontrolset\services\dps\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eaphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ehsched\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fax\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\gpsvc
Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\idsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ipbusenum
Opens key: HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lanmanserver
Opens key: HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\mmcss
Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msdtc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\napagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\

Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key: HKLM\system\currentcontrolset\services\netman
Opens key: HKLM\system\currentcontrolset\services\netman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netprofm
Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nlasvc
Opens key: HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nsi
Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ose\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pcasvc
Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\perfhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\plugplay
Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\power
Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\profsvc
Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\qwave
Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasauto\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpcss
Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\schedule
Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\seclogon\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sens
Opens key: HKLM\system\currentcontrolset\services\sens\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\sessionenv
Opens key: HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\spooler\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\stisvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\swprv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\tapisrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tbs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\termservice
Opens key: HKLM\system\currentcontrolset\services\termservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\themes
Opens key: HKLM\system\currentcontrolset\services\themes\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\threadorder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trkwks
Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\umrdpservice
Opens key: HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\uxsms
Opens key: HKLM\system\currentcontrolset\services\uxsms\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\w32time
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winmgmt
Opens key: HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
Opens key: HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\progid
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}
Opens key: HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCU\software\classes\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\progid
Opens key: HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler32
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\treatas
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\progid
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}
Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\progid
Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprochandler32
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler32
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprochandler
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\treatas
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treatas
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\progid
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}
Opens key: HKCR\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}
Opens key: HKCU\software\classes\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\progid
Opens key: HKCR\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\progid
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprocserver32
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprocserver32
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprochandler32
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprochandler32
Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprochandler
Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprochandler
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}
Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\treatas
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\treatas
Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\progid
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}
Opens key: HKCR\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}
Opens key: HKCU\software\classes\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\progid
Opens key: HKCR\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\progid
Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\inprocserver32
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprocserver32

Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprochandler32
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprochandler32
Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprochandler
Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprochandler
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\treatas
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\treatas
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
Opens key: HKCR\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
Opens key: HKCU\software\classes\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
Opens key: HKCR\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprocserver32
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprocserver32
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler32
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler32
Opens key: HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler
Opens key: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[859ba9477553ccad1bba34c555ab6a1b]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
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_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\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_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: 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\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[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\000000000008[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\000000000006[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\000000000004[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\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
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\000000000005[providerid]
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\000000000003[providerid]
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\000000000001[providerid]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[start]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[group]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\alg[imagepath]
Queries value: HKLM\system\currentcontrolset\services\alg[type]
Queries value: HKLM\system\currentcontrolset\services\alg[start]
Queries value: HKLM\system\currentcontrolset\services\alg[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\alg[tag]
Queries value: HKLM\system\currentcontrolset\services\alg[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\alg[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\alg[group]
Queries value: HKU\.default\control panel\desktop[preferreduilanguages]
Queries value: HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\system\currentcontrolset\services\alg[objectname]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[type]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[start]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[group]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\appinfo[imagepath]

Queries value: HKLM\system\currentcontrolset\services\appinfo[type]
Queries value: HKLM\system\currentcontrolset\services\appinfo[start]
Queries value: HKLM\system\currentcontrolset\services\appinfo[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\appinfo[tag]
Queries value: HKLM\system\currentcontrolset\services\appinfo[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\appinfo[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\appinfo[group]
Queries value: HKLM\system\currentcontrolset\services\appinfo[objectname]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[imagepath]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[type]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[start]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[tag]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[group]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[objectname]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[imagepath]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[type]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[start]
Queries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[tag]
Queries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[dependonservice]
Queries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[group]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[objectname]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[type]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[start]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[tag]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[group]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[objectname]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[type]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[start]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[tag]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[group]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[objectname]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[type]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[start]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[tag]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[cmd]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[group]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bfe[type]
Queries value: HKLM\system\currentcontrolset\services\bfe[start]
Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bfe[tag]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bfe[group]
Queries value: HKLM\system\currentcontrolset\services\bfe[objectname]
Queries value: HKLM\system\currentcontrolset\services\bits[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bits[type]
Queries value: HKLM\system\currentcontrolset\services\bits[start]
Queries value: HKLM\system\currentcontrolset\services\bits[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bits[tag]
Queries value: HKLM\system\currentcontrolset\services\bits[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bits[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bits[group]
Queries value: HKLM\system\currentcontrolset\services\bits[objectname]
Queries value: HKLM\system\currentcontrolset\services\bthserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bthserv[type]
Queries value: HKLM\system\currentcontrolset\services\bthserv[start]
Queries value: HKLM\system\currentcontrolset\services\bthserv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bthserv[tag]
Queries value: HKLM\system\currentcontrolset\services\bthserv[dependonservice]

Queries value: HKLM\system\currentcontrolset\services\bthserv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bthserv[group]
Queries value: HKLM\system\currentcontrolset\services\bthserv[objectname]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[imagepath]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[type]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[start]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[errorcontrol]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[tag]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[dependonservice]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[dependongroup]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[group]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[objectname]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[imagepath]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[type]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[start]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[errorcontrol]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[tag]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[dependonservice]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[dependongroup]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[group]
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[objectname]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[imagepath]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[type]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[start]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[tag]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[group]
Queries value: HKLM\system\currentcontrolset\services\comsysapp[objectname]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[type]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[start]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[group]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[type]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[start]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[tag]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[group]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[type]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[start]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[group]
Queries value: HKLM\system\currentcontrolset\services\defragsvc[objectname]
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\dot3svc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[type]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[start]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[tag]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[group]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[objectname]
Queries value: HKLM\system\currentcontrolset\services\eaphost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\eaphost[type]
Queries value: HKLM\system\currentcontrolset\services\eaphost[start]
Queries value: HKLM\system\currentcontrolset\services\eaphost[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\eaphost[tag]
Queries value: HKLM\system\currentcontrolset\services\eaphost[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\eaphost[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\eaphost[group]
Queries value: HKLM\system\currentcontrolset\services\eaphost[objectname]
Queries value: HKLM\system\currentcontrolset\services\efs[imagepath]
Queries value: HKLM\system\currentcontrolset\services\efs[type]
Queries value: HKLM\system\currentcontrolset\services\efs[start]
Queries value: HKLM\system\currentcontrolset\services\efs[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\efs[tag]
Queries value: HKLM\system\currentcontrolset\services\efs[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\efs[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\efs[group]
Queries value: HKLM\system\currentcontrolset\services\efs[objectname]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[type]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[start]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[tag]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[group]
Queries value: HKLM\system\currentcontrolset\services\ehrecvr[objectname]
Queries value: HKLM\system\currentcontrolset\services\ehsched[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ehsched[type]
Queries value: HKLM\system\currentcontrolset\services\ehsched[start]
Queries value: HKLM\system\currentcontrolset\services\ehsched[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ehsched[tag]
Queries value: HKLM\system\currentcontrolset\services\ehsched[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ehsched[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ehsched[group]
Queries value: HKLM\system\currentcontrolset\services\ehsched[objectname]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[imagepath]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[type]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[start]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[tag]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[group]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[objectname]
Queries value: HKLM\system\currentcontrolset\services\fax[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fax[type]
Queries value: HKLM\system\currentcontrolset\services\fax[start]
Queries value: HKLM\system\currentcontrolset\services\fax[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\fax[tag]
Queries value: HKLM\system\currentcontrolset\services\fax[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\fax[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\fax[group]
Queries value: HKLM\system\currentcontrolset\services\fax[objectname]
Queries value: HKLM\system\currentcontrolset\services\fdphost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fdphost[type]
Queries value: HKLM\system\currentcontrolset\services\fdphost[start]
Queries value: HKLM\system\currentcontrolset\services\fdphost[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\fdphost[tag]
Queries value: HKLM\system\currentcontrolset\services\fdphost[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\fdphost[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\fdphost[group]
Queries value: HKLM\system\currentcontrolset\services\fdphost[objectname]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[type]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[start]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[tag]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[group]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[objectname]
Queries value: HKLM\system\currentcontrolset\services\fontcache[imagepath]

Queries value: HKLM\system\currentcontrolset\services\fontcache[type]
Queries value: HKLM\system\currentcontrolset\services\fontcache[start]
Queries value: HKLM\system\currentcontrolset\services\fontcache[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\fontcache[tag]
Queries value: HKLM\system\currentcontrolset\services\fontcache[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\fontcache[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\fontcache[group]
Queries value: HKLM\system\currentcontrolset\services\fontcache[objectname]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[type]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[start]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[tag]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[group]
Queries value: HKLM\system\currentcontrolset\services\fontcache3.0.0.0[objectname]
Queries value: HKLM\system\currentcontrolset\services\hidserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\hidserv[type]
Queries value: HKLM\system\currentcontrolset\services\hidserv[start]
Queries value: HKLM\system\currentcontrolset\services\hidserv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\hidserv[tag]
Queries value: HKLM\system\currentcontrolset\services\hidserv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\hidserv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\hidserv[group]
Queries value: HKLM\system\currentcontrolset\services\hidserv[objectname]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[type]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[start]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[group]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[imagepath]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[type]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[start]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[tag]
Queries value:
HKLM\system\currentcontrolset\services\homegrouplistener[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[group]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[objectname]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[imagepath]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[type]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[start]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[tag]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[group]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[objectname]
Queries value: HKLM\system\currentcontrolset\services\idsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\idsvc[type]
Queries value: HKLM\system\currentcontrolset\services\idsvc[start]
Queries value: HKLM\system\currentcontrolset\services\idsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\idsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\idsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\idsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\idsvc[group]
Queries value: HKLM\system\currentcontrolset\services\idsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\keyiso[imagepath]
Queries value: HKLM\system\currentcontrolset\services\keyiso[type]
Queries value: HKLM\system\currentcontrolset\services\keyiso[start]
Queries value: HKLM\system\currentcontrolset\services\keyiso[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\keyiso[tag]
Queries value: HKLM\system\currentcontrolset\services\keyiso[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\keyiso[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\keyiso[group]
Queries value: HKLM\system\currentcontrolset\services\keyiso[objectname]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[type]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[start]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[tag]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[group]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[objectname]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[imagepath]

Queries value: HKLM\system\currentcontrolset\services\lltdsvc[type]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[start]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[group]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[type]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[start]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[tag]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[group]
Queries value: HKLM\system\currentcontrolset\services\mcx2svc[objectname]
Queries value: HKLM\system\currentcontrolset\services\msdtc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\msdtc[type]
Queries value: HKLM\system\currentcontrolset\services\msdtc[start]
Queries value: HKLM\system\currentcontrolset\services\msdtc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\msdtc[tag]
Queries value: HKLM\system\currentcontrolset\services\msdtc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\msdtc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\msdtc[group]
Queries value: HKLM\system\currentcontrolset\services\msdtc[objectname]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[imagepath]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[type]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[start]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[tag]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[group]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[objectname]
Queries value: HKLM\system\currentcontrolset\services\msiserver[imagepath]
Queries value: HKLM\system\currentcontrolset\services\msiserver[type]
Queries value: HKLM\system\currentcontrolset\services\msiserver[start]
Queries value: HKLM\system\currentcontrolset\services\msiserver[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\msiserver[tag]
Queries value: HKLM\system\currentcontrolset\services\msiserver[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\msiserver[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\msiserver[group]
Queries value: HKLM\system\currentcontrolset\services\msiserver[objectname]
Queries value: HKLM\system\currentcontrolset\services\napagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\napagent[type]
Queries value: HKLM\system\currentcontrolset\services\napagent[start]
Queries value: HKLM\system\currentcontrolset\services\napagent[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\napagent[tag]
Queries value: HKLM\system\currentcontrolset\services\napagent[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\napagent[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\napagent[group]
Queries value: HKLM\system\currentcontrolset\services\napagent[objectname]
Queries value: HKLM\system\currentcontrolset\services\netlogon[imagepath]
Queries value: HKLM\system\currentcontrolset\services\netlogon[type]
Queries value: HKLM\system\currentcontrolset\services\netlogon[start]
Queries value: HKLM\system\currentcontrolset\services\netlogon[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\netlogon[tag]
Queries value: HKLM\system\currentcontrolset\services\netlogon[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\netlogon[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\netlogon[group]
Queries value: HKLM\system\currentcontrolset\services\netlogon[objectname]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[imagepath]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[type]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[start]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[tag]
Queries value:
HKLM\system\currentcontrolset\services\nettcpportsharing[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[group]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[objectname]
Queries value: HKLM\system\currentcontrolset\services\ose[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ose[type]
Queries value: HKLM\system\currentcontrolset\services\ose[start]
Queries value: HKLM\system\currentcontrolset\services\ose[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ose[tag]
Queries value: HKLM\system\currentcontrolset\services\ose[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ose[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ose[group]
Queries value: HKLM\system\currentcontrolset\services\ose[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\p2psvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[type]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[start]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[tag]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[group]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[type]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[start]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[group]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\perfhost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\perfhost[type]
Queries value: HKLM\system\currentcontrolset\services\perfhost[start]
Queries value: HKLM\system\currentcontrolset\services\perfhost[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\perfhost[tag]
Queries value: HKLM\system\currentcontrolset\services\perfhost[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\perfhost[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\perfhost[group]
Queries value: HKLM\system\currentcontrolset\services\perfhost[objectname]
Queries value: HKLM\system\currentcontrolset\services\pla[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pla[type]
Queries value: HKLM\system\currentcontrolset\services\pla[start]
Queries value: HKLM\system\currentcontrolset\services\pla[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\pla[tag]
Queries value: HKLM\system\currentcontrolset\services\pla[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\pla[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\pla[group]
Queries value: HKLM\system\currentcontrolset\services\pla[objectname]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[type]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[start]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[group]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\policyagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\policyagent[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent[start]
Queries value: HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\policyagent[tag]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\policyagent[group]
Queries value: HKLM\system\currentcontrolset\services\policyagent[objectname]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[imagepath]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[type]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[start]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[tag]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[group]
Queries value: HKLM\system\currentcontrolset\services\protectedstorage[objectname]
Queries value: HKLM\system\currentcontrolset\services\rasauto[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rasauto[type]
Queries value: HKLM\system\currentcontrolset\services\rasauto[start]
Queries value: HKLM\system\currentcontrolset\services\rasauto[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\rasauto[tag]
Queries value: HKLM\system\currentcontrolset\services\rasauto[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\rasauto[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\rasauto[group]
Queries value: HKLM\system\currentcontrolset\services\rasauto[objectname]
Queries value: HKLM\system\currentcontrolset\services\rasman[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rasman[type]
Queries value: HKLM\system\currentcontrolset\services\rasman[start]
Queries value: HKLM\system\currentcontrolset\services\rasman[errorcontrol]

Queries value: HKLM\system\currentcontrolset\services\rasman[tag]
Queries value: HKLM\system\currentcontrolset\services\rasman[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\rasman[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\rasman[group]
Queries value: HKLM\system\currentcontrolset\services\rasman[objectname]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[imagepath]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[type]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[start]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[tag]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[group]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[objectname]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[imagepath]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[type]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[start]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[tag]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[group]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[type]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[start]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[tag]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[group]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[type]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[start]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[tag]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[group]
Queries value: HKLM\system\currentcontrolset\services\rpclocator[objectname]
Queries value: HKLM\system\currentcontrolset\services\samss[imagepath]
Queries value: HKLM\system\currentcontrolset\services\samss[type]
Queries value: HKLM\system\currentcontrolset\services\samss[start]
Queries value: HKLM\system\currentcontrolset\services\samss[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\samss[tag]
Queries value: HKLM\system\currentcontrolset\services\samss[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\samss[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\samss[group]
Queries value: HKLM\system\currentcontrolset\services\samss[objectname]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[imagepath]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[type]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[start]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[tag]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[group]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[objectname]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[type]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[start]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[tag]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[group]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[type]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[start]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[group]
Queries value: HKLM\system\currentcontrolset\services\sdrsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\seclogon[imagepath]
Queries value: HKLM\system\currentcontrolset\services\seclogon[type]
Queries value: HKLM\system\currentcontrolset\services\seclogon[start]
Queries value: HKLM\system\currentcontrolset\services\seclogon[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\seclogon[tag]
Queries value: HKLM\system\currentcontrolset\services\seclogon[dependonservice]

Queries value: HKLM\system\currentcontrolset\services\seclogon[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\seclogon[group]
Queries value: HKLM\system\currentcontrolset\services\seclogon[objectname]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[start]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[group]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[imagepath]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[type]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[start]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[tag]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[group]
Queries value: HKLM\system\currentcontrolset\services\snmptrap[objectname]
Queries value: HKLM\system\currentcontrolset\services\spooler[imagepath]
Queries value: HKLM\system\currentcontrolset\services\spooler[type]
Queries value: HKLM\system\currentcontrolset\services\spooler[start]
Queries value: HKLM\system\currentcontrolset\services\spooler[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\spooler[tag]
Queries value: HKLM\system\currentcontrolset\services\spooler[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\spooler[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\spooler[group]
Queries value: HKLM\system\currentcontrolset\services\spooler[objectname]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[type]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[start]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[group]
Queries value: HKLM\system\currentcontrolset\services\sppsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[type]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[start]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[tag]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[group]
Queries value: HKLM\system\currentcontrolset\services\sppuinotify[objectname]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[type]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[start]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[tag]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[group]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[type]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[start]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[group]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\stisvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\stisvc[type]
Queries value: HKLM\system\currentcontrolset\services\stisvc[start]
Queries value: HKLM\system\currentcontrolset\services\stisvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\stisvc[tag]
Queries value: HKLM\system\currentcontrolset\services\stisvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\stisvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\stisvc[group]
Queries value: HKLM\system\currentcontrolset\services\stisvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\storsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\storsvc[type]
Queries value: HKLM\system\currentcontrolset\services\storsvc[start]
Queries value: HKLM\system\currentcontrolset\services\storsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\storsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\storsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\storsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\storsvc[group]

Queries value: HKLM\system\currentcontrolset\services\storsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\swprv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\swprv[type]
Queries value: HKLM\system\currentcontrolset\services\swprv[start]
Queries value: HKLM\system\currentcontrolset\services\swprv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\swprv[tag]
Queries value: HKLM\system\currentcontrolset\services\swprv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\swprv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\swprv[group]
Queries value: HKLM\system\currentcontrolset\services\swprv[objectname]
Queries value: HKLM\system\currentcontrolset\services\sysmain[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sysmain[type]
Queries value: HKLM\system\currentcontrolset\services\sysmain[start]
Queries value: HKLM\system\currentcontrolset\services\sysmain[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sysmain[tag]
Queries value: HKLM\system\currentcontrolset\services\sysmain[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sysmain[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sysmain[group]
Queries value: HKLM\system\currentcontrolset\services\sysmain[objectname]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[type]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[start]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[tag]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[group]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[objectname]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[type]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[start]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[tag]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[group]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[objectname]
Queries value: HKLM\system\currentcontrolset\services\tbs[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tbs[type]
Queries value: HKLM\system\currentcontrolset\services\tbs[start]
Queries value: HKLM\system\currentcontrolset\services\tbs[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\tbs[tag]
Queries value: HKLM\system\currentcontrolset\services\tbs[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\tbs[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\tbs[group]
Queries value: HKLM\system\currentcontrolset\services\tbs[objectname]
Queries value: HKLM\system\currentcontrolset\services\threadorder[imagepath]
Queries value: HKLM\system\currentcontrolset\services\threadorder[type]
Queries value: HKLM\system\currentcontrolset\services\threadorder[start]
Queries value: HKLM\system\currentcontrolset\services\threadorder[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\threadorder[tag]
Queries value: HKLM\system\currentcontrolset\services\threadorder[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\threadorder[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\threadorder[group]
Queries value: HKLM\system\currentcontrolset\services\threadorder[objectname]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[type]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[start]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[tag]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[group]
Queries value: HKLM\system\currentcontrolset\services\tlntsvr[objectname]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[imagepath]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[type]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[start]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[tag]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[group]
Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[objectname]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[type]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[start]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[tag]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[group]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[objectname]

Queries value: HKLM\system\currentcontrolset\services\upnphost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\upnphost[type]
Queries value: HKLM\system\currentcontrolset\services\upnphost[start]
Queries value: HKLM\system\currentcontrolset\services\upnphost[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\upnphost[tag]
Queries value: HKLM\system\currentcontrolset\services\upnphost[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\upnphost[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\upnphost[group]
Queries value: HKLM\system\currentcontrolset\services\upnphost[objectname]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[type]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[start]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[group]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\vds[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vds[type]
Queries value: HKLM\system\currentcontrolset\services\vds[start]
Queries value: HKLM\system\currentcontrolset\services\vds[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\vds[tag]
Queries value: HKLM\system\currentcontrolset\services\vds[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\vds[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\vds[group]
Queries value: HKLM\system\currentcontrolset\services\vds[objectname]
Queries value: HKLM\system\currentcontrolset\services\vss[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vss[type]
Queries value: HKLM\system\currentcontrolset\services\vss[start]
Queries value: HKLM\system\currentcontrolset\services\vss[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\vss[tag]
Queries value: HKLM\system\currentcontrolset\services\vss[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\vss[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\vss[group]
Queries value: HKLM\system\currentcontrolset\services\vss[objectname]
Queries value: HKLM\system\currentcontrolset\services\wbengine[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wbengine[type]
Queries value: HKLM\system\currentcontrolset\services\wbengine[start]
Queries value: HKLM\system\currentcontrolset\services\wbengine[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wbengine[tag]
Queries value: HKLM\system\currentcontrolset\services\wbengine[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wbengine[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wbengine[group]
Queries value: HKLM\system\currentcontrolset\services\wbengine[objectname]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[type]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[start]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[group]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[type]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[start]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[group]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[type]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[start]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[tag]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[group]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[objectname]
Queries value: HKLM\system\currentcontrolset\services\webclient[imagepath]
Queries value: HKLM\system\currentcontrolset\services\webclient[type]
Queries value: HKLM\system\currentcontrolset\services\webclient[start]
Queries value: HKLM\system\currentcontrolset\services\webclient[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\webclient[tag]
Queries value: HKLM\system\currentcontrolset\services\webclient[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\webclient[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\webclient[group]
Queries value: HKLM\system\currentcontrolset\services\webclient[objectname]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[type]

Queries value: HKLM\system\currentcontrolset\services\wecsvc[start]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[group]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[type]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[start]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[tag]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[group]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[objectname]
Queries value: HKLM\system\currentcontrolset\services\wersvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wersvc[type]
Queries value: HKLM\system\currentcontrolset\services\wersvc[start]
Queries value: HKLM\system\currentcontrolset\services\wersvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wersvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wersvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wersvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wersvc[group]
Queries value: HKLM\system\currentcontrolset\services\wersvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\winrm[imagepath]
Queries value: HKLM\system\currentcontrolset\services\winrm[type]
Queries value: HKLM\system\currentcontrolset\services\winrm[start]
Queries value: HKLM\system\currentcontrolset\services\winrm[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\winrm[tag]
Queries value: HKLM\system\currentcontrolset\services\winrm[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\winrm[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\winrm[group]
Queries value: HKLM\system\currentcontrolset\services\winrm[objectname]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[type]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[start]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[group]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[type]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[start]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[tag]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[group]
Queries value: HKLM\system\currentcontrolset\services\wmiapsrv[objectname]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[type]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[start]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[group]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[type]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[start]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[group]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wsearch[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wsearch[type]
Queries value: HKLM\system\currentcontrolset\services\wsearch[start]
Queries value: HKLM\system\currentcontrolset\services\wsearch[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wsearch[tag]
Queries value: HKLM\system\currentcontrolset\services\wsearch[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wsearch[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wsearch[group]
Queries value: HKLM\system\currentcontrolset\services\wsearch[objectname]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[type]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[start]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[errorcontrol]

Queries value: HKLM\system\currentcontrolset\services\wuauserv[tag]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[group]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[objectname]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[type]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[start]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[group]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[type]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[start]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[group]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[objectname]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[rundll32]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser[imagepath]
Queries value: HKLM\system\currentcontrolset\services\browser[type]
Queries value: HKLM\system\currentcontrolset\services\browser[start]
Queries value: HKLM\system\currentcontrolset\services\browser[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\browser[tag]
Queries value: HKLM\system\currentcontrolset\services\browser[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\browser[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\browser[group]
Queries value: HKLM\system\currentcontrolset\services\browser[objectname]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]

Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ikeext[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext[start]
Queries value: HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ikeext[tag]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ikeext[group]
Queries value: HKLM\system\currentcontrolset\services\ikeext[objectname]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]

Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}[]
Queries value: HKCR\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprocserver32[]
Queries value: HKCR\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e0a40b26-30c4-4656-
bc9a-74a5c3a0b2ec]
Queries value: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}[]
Queries value: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprocserver32[]
Queries value: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}[]
Queries value: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprocserver32[]
Queries value: HKCR\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-

409d6c4515e9}\inprocserver32[]
Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
Value changes: HKLM\system\currentcontrolset\services\browser[start]
Value changes: HKLM\system\currentcontrolset\services\policyagent[start]