COM Telemetry

winreg Interface

Interface UUID: `338CD001-2244-31F1-AAAA-900038001003`

OpNum	Method Name
0	`OpenClassesRoot`
1	`OpenCurrentUser`
2	`OpenLocalMachine`
3	`OpenPerformanceData`
4	`OpenUsers`
5	`BaseRegCloseKey`
6	`BaseRegCreateKey`
7	`BaseRegDeleteKey`
8	`BaseRegDeleteValue`
9	`BaseRegEnumKey`
10	`BaseRegEnumValue`
11	`BaseRegFlushKey`
12	`BaseRegGetKeySecurity`
13	`BaseRegLoadKey`
14	`Opnum14NotImplemented`
15	`BaseRegOpenKey`
16	`BaseRegQueryInfoKey`
17	`BaseRegQueryValue`
18	`BaseRegReplaceKey`
19	`BaseRegRestoreKey`
20	`BaseRegSaveKey`
21	`BaseRegSetKeySecurity`
22	`BaseRegSetValue`
23	`BaseRegUnLoadKey`
24	`Opnum24NotImplemented`

OpNum	Method Name
25	`Opnum25NotImplemented`
26	`BaseRegGetVersion`
27	`OpenCurrentConfig`
28	`Opnum28NotImplemented`
29	`BaseRegQueryMultipleValues`
30	`Opnum30NotImplemented`
31	`BaseRegSaveKeyEx`
32	`OpenPerformanceText`
33	`OpenPerformanceNlsText`
34	`BaseRegQueryMultipleValues2`
35	`BaseRegDeleteKeyEx`

Reference: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rrp/47f3edf6-4c2d-45d8-ab5b-2dc077738903

wscapi interface

Interface UUID: `06bba54a-be05-49f9-b0a0-30f790261023`
DLL: `c:\windows\system32\wscsvc.dll`

OpNum	Function Name
0	`CWindowsFirewallDetectoid::OnResetWaitHandle`
1	`s_wscRegisterChangeNotification`
2	`s_wscUnRegisterChangeNotification`
3	`s_wscGetAlertStatus`
4	`s_wscAntiVirusExpiredBeyondThreshold`
5	`s_wscAntiVirusExpiredBeyondThreshold`
6	`s_wscAntiVirusExpiredBeyondThreshold`
7	`s_wscFirewallGetStatus`
8	`s_wscIcfEnable`
9	`s_wscAntiVirusGetStatus`
10	`s_wscAntiSpywareGetStatus`
11	`s_wscGeneralSecurityGetStatus`

OpNum	Function Name
12	`s_wscLuaSettingsFix`
13	`s_wscRegisterSecurityProduct`
14	`s_wscUnregisterSecurityProduct`
15	`s_wscUpdateProductStatus`
16	`s_wscAntiVirusExpiredBeyondThreshold`
17	`s_wscIsDefenderAntivirusSupported`
18	`s_wscUserNotificationRequired`
19	`s_wscInitiateOfflineCleaning`
20	`s_wscAbortOfflineCleaning`
21	`s_wscNotifyUserForNearExpiration`
22	`s_wscAntiVirusGetUpgradableProducts`
23	`s_wscAntiVirusRemoveUpgradableProduct`
24	`s_wscAntiVirusGetRemovedButNotUpgradableProducts`
25	`s_wscMakeDefaultProductRequest`
26	`s_wscSetDefaultProduct`
27	`s_wscUpdateProductSubStatus`

Source: https://gist.github.com/enigma0x3/092da9f249499391adffe2c46abfa1a1#file-rpc_dump_august-txt-L336

SspiSrv Interface

Interface UUID: `4f32adc8-6052-4a04-8701-293ccf2096f0`
DLL: `C:\WINDOWS\SYSTEM32\SspiSrv.dll`

OpNum	Function Name
0	`SspirConnectRpc`
1	`SspirDisconnectRpc`
2	`SspirDisconnectRpc`
3	`SspirCallRpc`
4	`SspirAcquireCredentialsHandle`
5	`SspirFreeCredentialsHandle`
6	`SspirProcessSecurityContext`

OpNum	Function Name
7	`SspirDeleteSecurityContext`
8	`SspirSslQueryCredentialsAttributes`
9	`SspirNegQueryContextAttributes`
10	`SspirSslSetCredentialsAttributes`
11	`SspirApplyControlToken`
12	`SspirLogonUser`
13	`SspirLookupAccountSid`
14	`SspirGetUserName`
15	`SspirGetInprocDispatchTable`

Source: https://gist.github.com/masthoon/510dd757b21f04da47431e9d4e0a3f6e

samsrv Interface

Interface UUID: `12345778-1234-abcd-ef00-0123456789ac`
DLL: `C:\WINDOWS\SYSTEM32\samsrv.dll`

OpNum	Function Name
0	`SamrConnect`
1	`SamrCloseHandle`
2	`SamrSetSecurityObject`
3	`SamrQuerySecurityObject`
4	`SamrShutdownSamServer`
5	`SamrLookupDomainInSamServer`
6	`SamrEnumerateDomainsInSamServer`
7	`SamrOpenDomain`
8	`SamrQueryInformationDomain`
9	`SamrSetInformationDomain`
10	`SamrCreateGroupInDomain`
11	`SamrEnumerateGroupsInDomain`
12	`SamrCreateUserInDomain`
13	`SamrEnumerateUsersInDomain`
14	`SamrCreateAliasInDomain`

OpNum	Function Name
15	`SamrEnumerateAliasesInDomain`
16	`SamrGetAliasMembership`
17	`SamrLookupNamesInDomain`
18	`SamrLookupIdsInDomain`
19	`SamrOpenGroup`
20	`SamrQueryInformationGroup`
21	`SamrSetInformationGroup`
22	`SamrAddMemberToGroup`
23	`SamrDeleteGroup`
24	`SamrRemoveMemberFromGroup`
25	`SamrGetMembersInGroup`
26	`SamrSetMemberAttributesOfGroup`
27	`SamrOpenAlias`
28	`SamrQueryInformationAlias`
29	`SamrSetInformationAlias`
30	`SamrDeleteAlias`
31	`SamrAddMemberToAlias`
32	`SamrRemoveMemberFromAlias`
33	`SamrGetMembersInAlias`
34	`SamrOpenUser`
35	`SamrDeleteUser`
36	`SamrQueryInformationUser`
37	`SamrSetInformationUser`
38	`SamrChangePasswordUser`
39	`SamrGetGroupsForUser`
40	`SamrQueryDisplayInformation`
41	`SamrGetDisplayEnumerationIndex`
42	`SamrTestPrivateFunctionsDomain`
43	`SamrTestPrivateFunctionsUser`
44	`SamrGetUserDomainPasswordInformation`
45	`SamrRemoveMemberFromForeignDomain`

OpNum	Function Name
46	`SamrQueryInformationDomain2`
47	`SamrQueryInformationUser2`
48	`SamrQueryDisplayInformation2`
49	`SamrGetDisplayEnumerationIndex2`
50	`SamrCreateUser2InDomain`
51	`SamrQueryDisplayInformation3`
52	`SamrAddMultipleMembersToAlias`
53	`SamrRemoveMultipleMembersFromAlias`
54	`SamrOemChangePasswordUser2`
55	`SamrUnicodeChangePasswordUser2`
56	`SamrGetDomainPasswordInformation`
57	`SamrConnect2`
58	`SamrSetInformationUser2`
59	`SamrSetBootKeyInformation`
60	`SamrGetBootKeyInformation`
61	`SamrConnect3`
62	`SamrConnect4`
63	`SamrUnicodeChangePasswordUser3`
64	`SamrConnect5`
65	`SamrRidToSid`
66	`SamrSetDSRMPassword`
67	`SamrValidatePassword`
68	`SamrQueryLocalizableAccountsInDomain`
69	`SamrPerformGenericOperation`
70	`SamrSyncDSRMPasswordFromAccount`
71	`SamrLookupNamesInDomain2`
72	`SamrEnumerateUsersInDomain2`

Source: https://gist.github.com/masthoon/510dd757b21f04da47431e9d4e0a3f6e#file-rpc_dump_rs4-txt-L366

efslsaext Interface

Interface UUID: `c681d488-d850-11d0-8c52-00c04fd90f7e`
DLL: `C:\WINDOWS\system32\efslsaext.dll`

OpNum	Function Name
0	`EfsRpcOpenFileRaw_Downlevel`
1	`EfsRpcReadFileRaw_Downlevel`
2	`EfsRpcWriteFileRaw_Downlevel`
3	`EfsRpcCloseRaw_Downlevel`
4	`EfsRpcEncryptFileSrv_Downlevel`
5	`EfsRpcDecryptFileSrv_Downlevel`
6	`EfsRpcQueryUsersOnFile_Downlevel`
7	`EfsRpcQueryRecoveryAgents_Downlevel`
8	`EfsRpcRemoveUsersFromFile_Downlevel`
9	`EfsRpcAddUsersToFile_Downlevel`
10	`EfsRpcFileKeyInfoEx_Downlevel`
11	`EfsRpcFileKeyInfoEx_Downlevel`
12	`EfsRpcFileKeyInfo_Downlevel`
13	`EfsRpcDuplicateEncryptionInfoFile_Downlevel`
14	`EfsRpcFileKeyInfoEx_Downlevel`
15	`EfsRpcAddUsersToFileEx_Downlevel`
16	`EfsRpcFileKeyInfoEx_Downlevel`
17	`EfsRpcFileKeyInfoEx_Downlevel`
18	`EfsRpcFileKeyInfoEx_Downlevel`
19	`EfsRpcFileKeyInfoEx_Downlevel`
20	`EfsRpcFlushEfsCache_Downlevel`