KEY Match Types

|  |  |  |  |
| --- | --- | --- | --- |
| Match Type Value | Description | Data type | Possible Values |
| ACCESS\_MASK | Specifies the access type. | UINT64 – BITMASK | **CREATE** (Key is  created)  **DELETE** (Key (not registry values)  is deleted or set security is  called)  **ENUM** (Key is opened with  KEY\_ENUMERATE  \_SUB\_KEYS)  **LOAD\_KEY** (Registry hive is loaded into a key  with ZwLoadKey or RegLoadKey.)  **QUERY** (Attempt to query a registry key occurs)  **READ** (Existing file/key is being opened  for read access)  **RENAME** (Registry key rename  operation occurs)  **REPLACE\_KEY** (Registry key is replaced using RegReplaceKey)  **RESTORE\_KEY** (Registry key is restored using RegRestoreKey)  **WRITE** (Existing key is opened for write using KEY\_WRITE) |
| OBJECT\_NAME | Specifies the object  name. Any combination  of wildcards is  accepted. | STRING |  |
| AUTHENTICATION\_ID | Matches a textual  account SDDL SID  identifier. This match  can be used to identify  a specific user-account  in policy enforcement. | STRING |  |
| NT\_ACCESS\_MASK | Matches against the  native NT access mask  of the I/O operation  for file, registry,  process, and thread  access attempts. Make  sure to use access  masks appropriate for  the object type as  described in Microsoft  MSDN.  For example, to  use NT\_ACCESS\_MASK  to block calls  to CreateFile() with  GENERIC\_WRITE, the  bit mask must be  FILE\_GENERIC\_WRITE. | UINT64 - BITMASK |  |
| OS\_VERSION | Compares the specified  operating system  version to the actual  version. The operating  system version must be  specified in the format:  OS\_Version =  Major\_Version \* 1000  + Minor\_Version \* 10  + ServicePack. By way  of example: VistaRtm  = 6000; VistaSp1=6001;  Win7=6010;  Win7Sp1=6011;  Win8=6020 | UINT32 |  |
| REGVAL\_DATA | Matches against  registry value data in  the context of a registry  value set operation,  either when a registry  variable is created or its  value is changed.  You can use this  MATCH\_type value to  control or filter the  data being written or  changed in a registry  value. | This data type is  variable. You must  specify it using the -type  flag.  Valid data types are the  same as accepted by  the Windows registry:   * INT32 * INT64 * BINARY * STRING * MULTI\_STRING * EXPANDABLE\_STRING |  |