

SetObjectSecurity v1.0

Local Security Descriptor Utility

SetObjectSecurity.exe enables you to set the security descriptor for just about any type of Windows securable object (files, directories, registry keys, event logs, services, SMB shares, etc). For file system and registry objects, you can choose whether to apply inheritance rules. You can also choose to output the security descriptor in a .reg-file-compatible representation of the security descriptor for a REG_BINARY registry value.

Use cases include:

- Restoring default security descriptor on the file system root directory (which sometimes gets misconfigured by some system setup tools)
- Restricting access to sensitive event logs that grant access too broadly (examples include AppLocker and PowerShell script block logs that grant read or read-write to NT AUTHORITY\INTERACTIVE)
- Locking down (or opening access to) file shares, directories, registry keys

SetObjectSecurity.exe is a 32-bit standalone executable that needs no installer, has no dependencies on redistributable DLLs, and works on all supported x86 and x64 versions of Windows. (x64 systems must support WOW64)

The command-line syntax for this mode is:

SetObjectSecurity.exe objType objName SDDL [...]

objType	Values include: file, FILE, key, KEY, eventlog, printer, service, share, kobject, process, thread, or regbinary. (All-caps FILE or KEY uses pre-Windows 2000 APIs to avoid applying inheritance.)
objName	The name of the object (quoted if it contains spaces); or a Process ID (PID) or Thread ID (TID) in decimal if objType is "process" or "thread"; or a registry value name if objType is "regbinary"
SDDL	The security descriptor to apply, in Security Descriptor Definition Language
-v	Reports verbose diagnostic output to stderr (optional)
-q	Do not display the startup banner and copyright message (optional)

Run SetObjectSecurity without parameters to see the full syntax and examples.

Use Windows Sysinternals [AccessChk](#) with the -L switch to get the SDDL representing an object's current security descriptor.