








| | | | | | | |
|---|---|--|--|--|--|--|
| SeAssignPrimaryTokenPrivilege | SeAuditPrivilege |  SeBackupPrivilege | SeChangeNotifyPrivilege | SeCreateGlobalPrivilege | SeCreatePagefilePrivilege | SeCreatePermanentPrivilege |
| Replace a process-level token. | Generate security audit. | Backup file and directories. | Bypass traverse checking. | Create global objects. | Create a pagefile. | Create permanent shared objects. |
| Checked by various components, such as <code>NtSetInformationJobObject</code> , that set a process's token. | Required to generate events for the Security event log with the <code>ReportEvent</code> API. | Grant the following access to any file or directory: <code>READ_CONTROL</code> , <code>ACCESS_SYSTEM_SECURITY</code> , <code>FILE_GENERIC_READ</code> , <code>FILE_TRAVERSE</code> . | Avoid checking permissions on intermediate directories of a multilevel directory lookup. | Required for a process to create section and symbolic link objects in the directories of the object manager namespace. | Checked by <code>NtCreatePagingFile</code> , which is the function used to create a new paging file. | Checked by the object manager when creating a permanent object. |
| SeCreateSymbolicLinkPrivilege |  SeCreateTokenPrivilege | SeManageVolumePrivilege | SeEnableDelegationPrivilege |  SeImpersonatePrivilege | SeIncreaseBasePriorityPrivilege | SeIncreaseQuotaPrivilege |
| Create symbolic links. | Create a token object. | Perform volume maintenance tasks. | Enable computer and user accounts to be trusted for delegation. | Impersonate a client after authentication. | Increase scheduling priority. | Adjust memory quotas for a process. |
| Checked by NTFS when creating symbolic links with the <code>CreateSymbolicLink</code> API. | Checked by <code>NtCreateToken</code> to create a token object. | Enforced by file system drivers during a volume open operation, which is required to perform disk-checking. | Used by Active Directory services to delegate authenticated credentials. | Process manager checks for this when a thread wants to use a token for impersonation. | Checked by the process manager and is required to raise the priority of a process. | Enforced when changing a process's working set thresholds, a process's paged and nonpaged pool quotas, and a process's CPU rate quota. |

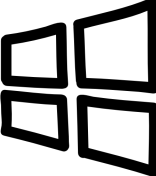
| | |
|---|--|
| SeIncreaseWorkingSetPrivilege |  SeLoadDriverPrivilege |
| Increase a process working set. | Load and unload device drivers. |
| Required to call <code>SetProcessWorkingSetSize</code> to increase the minimum working set. | Checked by <code>NtLoadDriver</code> and <code>NtUnloadDriver</code> driver functions. |


| | |
|--|--|
| SeProfileSingleProcessPrivilege |  SeDebugPrivilege |
| Profile single process. | Debug programs. |
| Checked by Superfetch and the prefetcher when requesting information for an individual process through <code>NtQuerySystemInformation</code> . | If the caller has this privilege enabled, the process manager allows access to any process or thread using <code>NtOpenProcess</code> or <code>NtOpenThread</code> , regardless the security descriptor. |

| | |
|---|--|
| SeShutdownPrivilege | SeSecurityPrivilege |
| Shutdown the system. | Manage auditing and security log. |
| Checked by <code>NtShutdownSystem</code> and <code>NtRaiseHardError</code> , which presents a system error dialog box on the interactive console. | Required to access the SACL of a security descriptor and to read and clear the security event log. |

| | |
|---|---|
|  SeTrustedCredManAccessPrivilege |  SeTcbPrivilege |
| Access Credential Manager as a trusted caller. | Act as part of the operating system. |
| Checked by the Credential Manager to verify that it should trust the caller with credential information that can be queried in plaintext. | Checked by the SRM when the session ID is set in a token, by the Plug and Play manager for Plug and Play event creation and management. |

WINDOWS PRIVILEGES



 Commonly abused privileges

| |
|--|
|  SeRestorePrivilege |
| Restore files and directories. |
| Grant access to any file or directory, regardless of the security descriptor that's present: <code>WRITE_DAC</code> , <code>WRITE_OWNER</code> , <code>ACCESS_SYSTEM_SECURITY</code> , <code>FILE_GENERIC_WRITE</code> , <code>FILE_ADD_FILE</code> , <code>FILE_ADD_SUBDIRECTORY</code> and <code>DELETE</code> . |

| |
|--|
| SeSyncAgentPrivilege |
| Synchronize directory service data. |
| Required to use the LDAP directory synchronization services. It allows the holder to read all objects and properties in the directory. |

| |
|--|
| SeSystemEnvironmentPrivilege |
| Modify firmware environment variables. |
| Required by <code>NtSetSystemEnvironmentValue</code> and <code>NtQuerySystemEnvironmentValue</code> to modify and read firmware environment variables using the HAL. |

| |
|---|
| SeLockMemoryPrivilege |
| Lock pages in memory. |
| Checked by <code>NtLockVirtualMemory</code> , the kernel implementation of <code>VirtualLock</code> . |

| |
|---|
| SeRelabelPrivilege |
| Modify an object label. |
| Checked by the SRM when raising the integrity level of an object owned by another user. |

| |
|---|
| SeSyncAgentPrivilege |
| Profile system performance. |
| Checked for by <code>NtCreateProfile</code> , the function used to perform profiling of the system. This is used by the Kernprof tool, for example. |

| |
|--|
| SeMachineAccountPrivilege |
| Add workstations to the domain. |
| Checked by the SAM on a domain controller when creating a machine account in a domain. |

| |
|--|
| SeRemoteShutdownPrivilege |
| Force shutdown from a remote system. |
| Winlogon checks that remote callers of the <code>InitiateSystemShutdown</code> function have this privilege. |

| |
|--------------------------------------|
| SeSystemtimePrivilege |
| Change the system time. |
| Required to change the time or date. |

| |
|---|
|  SeTakeOwnershipPrivilege |
| Take ownership of files and other objects. |
| Required to take ownership of an object without being granted discretionary access. |

| |
|---|
| SeUndockPrivilege |
| Remove computer from a docking station. |
| Checked by the user-mode Plug and Play manager when a computer undock is initiated. |

| |
|--|
| SeUnsolicitedInputPrivilege |
| Receive unsolicited data from a terminal device. |
| This privilege is not currently used by Windows. |