Access-Control Entry (ACE) Flags and Inheritance Rules

CONTAINER_INHERIT_ACE:

Child objects that are containers, such as directories, inherit the ACE as an effective ACE. The inherited ACE is inheritable unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.

INHERIT_ONLY_ACE:
This flag indicates an inherit-only ACE that doesn't control access to the object it's attached to.

INHERITED_ACE:

This flag indicates that the ACE was inherited. The system sets this bit when it propagates an inheritable ACE to a child object.

NO_PROPAGATE_INHERIT_ACE:

If the ACE is inherited by a child object, the system clears the OBJECT_INHERIT_ACE and CONTAINER_INHERIT_ACE flags in the inherited ACE. This action prevents the ACE from being inherited by subsequent generations of objects.

OBJECT_INHERIT_ACE:

Non-container child objects inherit the ACE as an effective ACE. For objects that are containers, the ACE is inherited as an inherit-only ACE unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.

OTHER CONSIDERATIONS:

In NT 4.0, objects only inherit ACEs from a parent container (e.g., registry key or directory) when they are created.

- No distinction is made between inherited and non-inherited ACEs
- No prevention of inheritance

In Windows 2000 and higher, inheritance is controllable

- SetNamedSecurityInfoEx and SetSecurityInfoEx
- Will apply new inheritable ACEs to all child objects (subkeys, files)
- Directly applied ACEs take precedence over inherited ACEs

RECOMMENDED INTERNET SITES:

How Permissions Work

https://web.archive.org/web/20181219185231/https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.