NTFS General Info Data Recovery Software FAQ Contacts Site Map Privacy & Terms About Us

NTFS General Information > NTFS Permissions > Access Control Entries

Access Control Entries

As stated previously, an ACL (Access Control List) is an ordered list of ACEs (Access Control Entries). Each ACE contains the following:

- A SID (Security Identifier) that identifies a particular user or group.
- An access mask that specifies access rights.
- A set of bit flags that determine whether or not child objects can inherit the ACE.
- A flag that indicates the type of ACE.

ACEs are fundamentally alike. What sets them apart is the degree of control they offer over inheritance and object access. There are two types of ACE:

- Generic type that are attached to all securable objects.
- Object-specific type that can occur only in ACLs for Active Directory objects.

Generic ACE

A generic ACE offers limited control over the kinds of child objects that can inherit them. Essentially, they can distinguish only between containers and noncontainers.

For example, the DACL (Discretionary Access Control List) on a Folder object in NTFS can include a generic ACE that allows a group of users to list the folder's contents. Because listing a folder's contents is an operation that can be performed only on a Container object, the ACE that allows the operation can be flagged as a CONTAINER_INHERIT_ACE. Only Container objects in the folder (that is, only other Folder objects) inherit the ACE. Noncontainer objects (that is, File objects) do not inherit the ACE of the parent object.

A generic ACE applies to an entire object. If a generic ACE gives a particular user Read access, the user can read all the information that is associated with the object — both data and properties. This is not a serious limitation for most object types. File objects, for example, have few properties, which are all used for describing characteristics of the object rather than for storing information. Most of the information in a File object is stored as object data; therefore, there is little need for separate controls on a file's properties.

Object-specific ACE

An object-specific ACE offers a greater degree of control over the types of child objects that can inherit them.

For example, an OU (Organizational Unit) object's ACL can have an object-specific ACE that is marked for inheritance only by User objects. Other types of objects, such as Computer objects, will not inherit the ACE.

This capability is why object-specific ACEs are called object-specific. Their inheritance can be limited to specific types of child objects.

There are similar differences in how the two categories of ACE types control access to objects.

An object-specific ACE can apply to any individual property of an object or to a set of properties for that object. This type of ACE is used only in an ACL for Active Directory objects, which, unlike other object types, store most

- NTFS Permissions
  - Setting Permissions
  - File and Folder Basic Permissions
  - File and Folder Advanced Permissions
  - Effective Permissions
  - Changing Ownership of Files and Folders
  - Moving and Copying Protected Files
  - Troubleshooting Access to Files and Shared Folders
  - Permissions for Other Objects
  - User Rights vs. NTFS Permissions
  - Share Permissions vs. NTFS Permissions
  - Explicit vs. Inherited Permissions
  - Allow vs. Deny Permissions
  - Permission Precedence
  - Combining Shared Folder Permissions and NTFS Permissions
  - Sharing and Adding Permissions
  - Backing up and Restoring NTFS Permissions on a Specified Volume
  - Off-line Access to Shared Folders (Caching)
- Metafile $Secure
  - A Brief History of NTFS
  - Structure of $Secure File
  - NTFS Security Descriptor
  - Access Control Lists in the Security Descriptor
  - How the System Uses ACLs
  - ✓ Access Control Entries
  - Security Identifier
- Appendix. Script to Backup or Restore

of their information in properties. It is often desirable to place independent controls on each property of an Active Directory object, and object-specific ACEs make that possible.

For example, when you define permissions for a User object, you can use one object-specific ACE to allow Principal Self (that is, the user) Write access to the Phone-Home-Primary (homePhone) property, and you can use other object-specific ACEs to deny Principal Self access to the Logon-Hours (logonHours) property and other properties that set restrictions on the user account.

The table below shows the layout of each ACE.

Access Control Entry Layout

ACE Field	Description
Type	Flag that indicates the type of ACE. Windows 2000 and Windows Server 2003 support six types of ACE: - Three generic ACE types that are attached to all securable objects. - Three object-specific ACE types that can occur for Active Directory objects.
Flags	Set of bit flags that control inheritance and auditing.
Size	Number of bytes of memory that are allocated for the ACE.
Access mask	32-bit value whose bits correspond to access rights for the object. Bits can be set either on or off, but the setting's meaning depends on the ACE type. For example, if the bit that corresponds to the right to read permissions is turned on, and the ACE type is Deny, the ACE denies the right to read the object's permissions. If the same bit is set on but the ACE type is Allow, the ACE grants the right to read the object's permissions. More details of the Access mask appear in the next table.
SID	Identifies a user or group whose access is controlled or monitored by this ACE.

Access Mask Layout

Bit (Range)	Meaning	Description/Example
0 - 15	Object Specific Access Rights	Read data, Execute, Append data
16 - 22	Standard Access Rights	Delete, Write ACL, Write Owner
23	Can access security ACL	
24 - 27	Reserved	
28	Generic ALL (Read, Write, Execute)	Everything below
29	Generic Execute	All things necessary to execute a program

NTFS Permissions
- Glossary

30	Generic Write	All things necessary to write to a file
31	Generic Read	All things necessary to read a file

Previous | NTFS Permissions | Next

Data Recovery

UNFORMAT
Active@ UNERASER
Active@ UNDELETE
Active@ File Recovery
Active@ Partition Recovery
Active@ Password Changer

Disk Utilities

Active@ Boot Disk(Live CD)
Active@ Partition Manager
Active@ Hard Disk Monitor
NTFS Reader for DOS
Active@ Disk Editor
NTFS Recovery toolkit

Data Security

Active@ KillDisk
Active@ ERASER
Active@ ZDelete
Active@ ZDelete Network

Data Backup

Active@ Disk Image

Data CD/DVD

Active@ ISO File Manager
Active@ ISO Burner
Active@ Data Burner
Active@ DVD Eraser

Be with us Follow us Look for us Contact us