

Aby wyświetlić następujące informacje o składni, wpisz `icacls.exe /?` w wierszu polecenia.

`ICACLS name /save aclfile [/T] [/C]` store the acls for all matching names into aclfile for later use with `/restore`.

`ICACLS directory [/substitute SidOld SidNew [...]] /restore aclfile [/C]`
applies the stored acls to files in directory.

`ICACLS name /setowner user [/T] [/C]`
changes the owner of all matching names.

`ICACLS name /findsid Sid [/T] [/C]`
finds all matching names that contain an ACL explicitly mentioning Sid.

`ICACLS name /verify [/T] [/C]`
finds all files whose ACL is not in canonical form or whose lengths are inconsistent with ACE counts.

`ICACLS name /resize [/T] [/C] [/L]`
changes incorrect recorded lengths of ACLs to true lengths.

`ICACLS name /reset [/T] [/C]`
replaces acls with default inherited acls for all matching files.

`ICACLS name [/grant[:r] Sid:perm[...]]`
`[/deny Sid:perm [...]]`
`[/remove[:g:d]] Sid[...]] [/T] [/C]`

`/grant[:r] Sid:perm` grants the specified user access rights. With `:r`, the permissions replace any previously granted explicit permissions. Without `:r`, the permissions are added to any previously granted explicit permissions.

`/deny Sid:perm` explicitly denies the specified user access rights.

An explicit deny ACE is added for the stated permissions and the same permissions in any explicit grant are removed.

/remove[:[g|d]] Sid removes all occurrences of Sid in the acl. With :g, it removes all occurrences of granted rights to that Sid. With :d, it removes all occurrences of denied rights to that Sid.

Note:

Sids may be in either numeric or friendly name form. If a numeric form is given, affix a * to the start of the SID.

/T indicates that this operation is performed on all matching files/directories below the directories specified in the name.

/C indicates that this operation will continue on all file errors. Error messages will still be displayed.

ICACLS preserves the canonical ordering of ACE entries:

- Explicit denials
- Explicit grants
- Inherited denials
- Inherited grants

perm is a permission mask and can be specified in one of two forms:

a sequence of simple rights:

- F - full access
- M - modify access
- RX - read and execute access
- R - read-only access
- W - write-only access

a comma-separated list in parentheses of specific rights:

- D - delete
- RC - read control

WDAC - write DAC
WO - write owner
S - synchronize
AS - access system security
MA - maximum allowed
GR - generic read
GW - generic write
GE - generic execute
GA - generic all
RD - read data/list directory
WD - write data/add file
AD - append data/add subdirectory
REA - read extended attributes
WEA - write extended attributes
X - execute/traverse
DC - delete child
RA - read attributes
WA - write attributes

inheritance rights may precede either form and are applied only to directories:

(OI) - object inherit
(CI) - container inherit
(IO) - inherit only
(NP) - don't propagate inherit

Examples:

```
icacls c:\windows\* /save AclFile /T
```

- Will save the ACLs for all files under c:\windows and its subdirectories to AclFile.

```
icacls c:\windows\ /restore AclFile
```

- Will restore the Acls for every file within AclFile that exists in c:\windows and its subdirectories

icacls file /grant Administrator:(D,WDAC)

- Will grant the user Administrator Delete and Write DAC permissions to file

icacls file /grant *S-1-1-0:(D,WDAC)

- Will grant the user defined by sid S-1-1-0 Delete and Write DAC permissions to file