AccessChk v6.14

Article • 06/22/2021 • 2 minutes to read • +1

Is this page helpful?

In this article

By Mark Russinovich

Published: June 22, 2021

Download AccessChk (958 KB)

Run now from Sysinternals Live .

Introduction

As a part of ensuring that they've created a secure environment Windows administrators often need to know what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows services. AccessChk quickly answers these questions with an intuitive interface and output.

Installation

AccessChk is a console program. Copy AccessChk onto your executable path. Typing "accesschk" displays its usage syntax.

Using AccessChk

Usage:

```
cmd
```

Copy

```
accesschk [-s][-e][-u][-r][-w][-n][-v]-[f <account>,...][[-a]|[-k]|[-p [-f] [-
t]]|[-h][-o [-t <object type>]][-c]|[-d]] [[-l [-i]]|[username]] <file, direc-
tory, registry key, process, service, object>
```

Parameter	Description
-a	Name is a Windows account right. Specify `"*"` as the name to show all rights assigned to a user. Note that when you specify a specific right, only groups and accounts directly assigned to the right are displayed.
-c	Name is a Windows Service, e.g. `ssdpsrv`. Specify `"*"` as the name to show all services and `scmanager` to check the security of the Service Control Manager.
-d	Only process directories or top-level keys
-e	Only show explicitly set-Integrity Levels (Windows Vista and higher only)
-f	If following `-p`, shows full process token information including groups and privileges. Otherwise is a list of comma-separated accounts to filter from the output.
-h	Name is a file or printer share. Specify `"*"` as the name to show all shares.
-i	Ignore objects with only inherited ACEs when dumping full access control lists.
-k	Name is a Registry key, e.g. `hklm\software`
-l	Show full security descriptor. Add `-i` to ignore inherited ACEs.
-n	Show only objects that have no access
-o	Name is an object in the Object Manager namespace (default is root). To view the contents of a directory, specify the name with a trailing backslash or add `-s`. Add `-t` and an object type (e.g. section) to see only objects of a specific type.
-p	Name is a process name or PID, e.g. `cmd.exe` (specify `"*"` as the name to show all processes). Add `-f` to show full process token information, including groups and privileges. Add `-t` to show threads.
-q	Omit Banner
-r	Show only objects that have read access

Parameter	Description
-s	Recurse
-t	Object type filter, e.g. `"section"`
-u	Suppress errors
-v	Verbose (includes Windows Vista Integrity Level)
-w	Show only objects that have write access

If you specify a user or group name and path, AccessChk will report the effective permissions for that account; otherwise it will show the effective access for accounts referenced in the security descriptor.

By default, the path name is interpreted as a file system path (use the `"\pipe\"` prefix to specify a named pipe path). For each object, AccessChk prints `R` if the account has read access, `W` for write access, and nothing if it has neither. The `-v` switch has AccessChk dump the specific accesses granted to an account.

Examples

The following command reports the accesses that the Power Users account has to files and directories in `\Windows\System32`:

cmd Copy

```
accesschk "power users" c:\windows\system32
```

This command shows which Windows services members of the Users group have write access to:

cmd Copy

```
accesschk users -cw *
```

To see what Registry keys under `HKLM\CurrentUser` a specific account has no access to:

cmd Copy

```
accesschk -kns austin\mruss hklm\software
```

To see the security on the HKLM\Software key:

cmd Copy

```
accesschk -k hklm\software
```

To see all files under `\Users\Mark` on Vista that have an explicit integrity level:

cmd Copy

```
accesschk -e -s c:\users\mark
```

To see all global objects that Everyone can modify:

cmd Copy

```
accesschk -wuo everyone \basednamedobjects
```

 **Download AccessChk** **(958 KB)**

Run now from Sysinternals Live .

Recommended content

Sysinternals Networking Utilities - Windows Sysinternals

Windows Sysinternals networking utilities

PsList - Windows Sysinternals

Show information about processes and threads.

Whois - Windows Sysinternals

See who owns an Internet address.

PsInfo - Windows Sysinternals

Obtain information about a system.

Show more