

# Sysinternals Security Utilities

## [AccessChk](#)

This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

## [AccessEnum](#)

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

## [Autologon](#)

Bypass password screen during logon.

## [Autoruns](#)

See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

## [LogonSessions](#)

List active logon sessions

## [Process Explorer](#)

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

## [PsExec](#)

Execute processes with limited-user rights.

## [PsLoggedOn](#)

Show users logged on to a system.

## [PsLogList](#)

Dump event log records.

## [PsTools](#)

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

## [Rootkit Revealer](#)

RootkitRevealer is an advanced rootkit detection utility.

### [SDelete](#)

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

### [ShareEnum](#)

Scan file shares on your network and view their security settings to close security holes.

### [ShellRunas](#)

Launch programs as a different user via a convenient shell context-menu entry.

### [Sigcheck](#)

Dump file version information and verify that images on your system are digitally signed.

### [Sysmon](#)

Monitors and reports key system activity via the Windows event log.

---

## Recommended content

- **[RootkitRevealer - Sysinternals](#)**  
Scan your system for rootkit-based malware.
- **[Sysinternals System Information Utilities - Windows Sysinternals](#)**  
Windows Sysinternals system information utilities
- **[Sysinternals Miscellaneous Utilities - Windows Sysinternals](#)**  
Windows Sysinternals miscellaneous utilities
- **[PsFile - Windows Sysinternals](#)**  
See what files are opened remotely.