## What is an access control list (ACL)?

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

Each system resource has a security attribute that identifies its access control list. The list includes an entry for every user who can access the system. The most common privileges for a file system ACL include the ability to read a file or all the files in a directory, to write to the file or files, and to execute the file if it is an executable file or program. ACLs are also built into network interfaces and operating systems (OSes), including Linux and Windows. On a computer network, access control lists are used to prohibit or allow certain types of traffic to the network. They commonly filter traffic based on its source and destination.

## What are access control lists used for?

Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device. Those devices can be network devices that act as network [gateways](https://internetofthingsagenda.techtarget.com/definition/gateway) or [endpoint devices](https://www.techtarget.com/whatis/definition/endpoint-device) that users access directly.

On a computer system, certain users have different levels of privilege, depending on their role. For example, a user logged in as network administrator may have read, write and edit permissions for a sensitive file or other resource. By contrast, a user logged in as a guest may only have read permissions.

Access control lists can help organize traffic to improve network efficiency and to give network administrators granular control over users on their computer systems and networks. ACLs can also be used to improve network security by keeping out malicious traffic.

## How do ACLs work?

Each ACL has one or more access control entries (ACEs) consisting of the name of a user or group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups or roles, the access privileges are stated in a string of [bits](https://www.techtarget.com/whatis/definition/bit-binary-digit) called an access mask. Generally, the system administrator or the object owner creates the access control list for an object.

## Types of access control lists

There are two basic types of ACLs:

1. **File system ACLs** manage access to files and directories. They give OSes the instructions that establish user access permissions for the system and their privileges once the system has been accessed.
2. **Networking ACLs** manage network access by providing instructions to network switches and routers that specify the types of traffic that are allowed to interface with the network. These ACLs also specify user permissions once inside the network. The network administrator predefines the networking ACL rules. In this way, they function similar to a [firewall](https://www.techtarget.com/searchsecurity/definition/firewall).

ACLs can also be categorized by the way they identify traffic:

* **Standard ACLs** block or allow an entire protocol suite using source [IP](https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol) addresses.
* **Extended ACLs** block or allow [network traffic](https://www.techtarget.com/searchnetworking/definition/network-traffic) based on a more differentiated set of characteristics that includes source and destination [IP addresses](https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address) and [port](https://www.techtarget.com/searchnetworking/definition/port) numbers, as opposed to just source address.