**Linux Pluggable Authentication Modules** (PAM) is a suite of libraries that allows a Linux [system administrator](https://en.wikipedia.org/wiki/System_administrator) to configure methods to [authenticate](https://en.wikipedia.org/wiki/Authentication) users. It provides a flexible and centralized way to switch authentication methods for secured applications by using configuration files instead of changing application code.[[1]](https://en.wikipedia.org/wiki/Linux_PAM#cite_note-1) There are Linux PAM libraries allowing authentication using methods such as local passwords, [LDAP](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol), or fingerprint readers.[[2]](https://en.wikipedia.org/wiki/Linux_PAM#cite_note-2) Linux PAM is evolved from the [Unix](https://en.wikipedia.org/wiki/Unix) [Pluggable Authentication Modules](https://en.wikipedia.org/wiki/Pluggable_Authentication_Modules) architecture.[[3]](https://en.wikipedia.org/wiki/Linux_PAM#cite_note-3)

Linux-PAM separates the tasks of authentication into four independent management groups:[[4]](https://en.wikipedia.org/wiki/Linux_PAM#cite_note-4)

* account modules check that the specified account is a valid authentication target under current conditions. This may include conditions like account expiration, time of day, and that the user has access to the requested service.
* authentication modules verify the user's identity, for example by requesting and checking a password or other secret. They may also pass authentication information on to other systems like a [keyring](https://en.wikipedia.org/wiki/Keyring_(cryptography)).
* password modules are responsible for updating passwords, and are generally coupled to modules employed in the authentication step. They may also be used to enforce strong passwords.
* session modules define actions that are performed at the beginning and end of sessions. A session starts after the user has successfully authenticated.