

**NAME**

pam\_limits – PAM module to limit resources

**SYNOPSIS**

**pam\_limits.so** [conf=*/path/to/limits.conf*] [debug] [set\_all] [utmp\_early] [noaudit]

**DESCRIPTION**

The pam\_limits PAM module sets limits on the system resources that can be obtained in a user-session. Users of *uid=0* are affected by this limits, too.

By default limits are taken from the */etc/security/limits.conf* config file. Then individual \*.conf files from the */etc/security/limits.d/* directory are read. The files are parsed one after another in the order of "C" locale. The effect of the individual files is the same as if all the files were concatenated together in the order of parsing. If a config file is explicitly specified with a module option then the files in the above directory are not parsed.

The module must not be called by a multithreaded application.

If Linux PAM is compiled with audit support the module will report when it denies access based on limit of maximum number of concurrent login sessions.

**OPTIONS**

**conf**=*/path/to/limits.conf*

Indicate an alternative limits.conf style configuration file to override the default.

**debug**

Print debug information.

**set\_all**

Set the limits for which no value is specified in the configuration file to the one from the process with the PID 1. Please note that if the init process is systemd these limits will not be the kernel default limits and this option should not be used.

**utmp\_early**

Some broken applications actually allocate a utmp entry for the user before the user is admitted to the system. If some of the services you are configuring PAM for do this, you can selectively use this module argument to compensate for this behavior and at the same time maintain system-wide consistency with a single limits.conf file.

**noaudit**

Do not report exceeded maximum logins count to the audit subsystem.

**MODULE TYPES PROVIDED**

Only the **session** module type is provided.

**RETURN VALUES**

PAM\_ABORT

Cannot get current limits.

PAM\_IGNORE

No limits found for this user.

PAM\_PERM\_DENIED

New limits could not be set.

PAM\_SERVICE\_ERR

Cannot read config file.

PAM\_SESSION\_ERR

Error recovering account name.

PAM\_SUCCESS

Limits were changed.

PAM\_USER\_UNKNOWN

The user is not known to the system.

## FILES

/etc/security/limits.conf

Default configuration file

## EXAMPLES

For the services you need resources limits (login for example) put a the following line in /etc/pam.d/login as the last line for that service (usually after the pam\_unix session line):

```
#%PAM-1.0
#
# Resource limits imposed on login sessions via pam_limits
#
session required pam_limits.so
```

Replace "login" for each service you are using this module.

## SEE ALSO

**limits.conf(5)**, **pam.d(5)**, **pam(7)**.

## AUTHORS

pam\_limits was initially written by Cristian Gafton <gafton@redhat.com>