



## ***Rocky Enterprise Linux 9.2 Manual Pages on command 'pam\_tally.8'***

**C:\>man pam\_tally.8**

PAM\_TALLY(8)                      Linux-PAM Manual                      PAM\_TALLY(8)

### NAME

pam\_tally - The login counter (tallying) module

### SYNOPSIS

```
pam_tally.so [file=/path/to/counter] [onerr=[fail|succeed]] [magic_root]
             [even_deny_root_account] [deny=n] [lock_time=n] [unlock_time=n]
             [per_user] [no_lock_time] [no_reset] [audit] [silent] [no_log_info]
pam_tally [--file /path/to/counter] [--user username] [--reset[=n]] [--quiet]
```

### DESCRIPTION

This module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail.

pam\_tally has several limitations, which are solved with pam\_tally2. For this reason pam\_tally is deprecated and will be removed in a future release.

pam\_tally comes in two parts: pam\_tally.so and pam\_tally. The former is the PAM module and the latter, a stand-alone program. pam\_tally is an (optional) application which can be used to interrogate and manipulate the counter file. It can display user counts, set individual counts, or clear all counts. Setting artificially high counts may be useful for blocking users without changing their passwords. For example, one might find it useful to clear all counts every midnight from a cron job. The faillog(8) command can be used instead of pam\_tally to maintain the counter file.

Normally, failed attempts to access root will not cause the root account to become

blocked, to prevent denial-of-service: if your users aren't given shell accounts and root may only login via su or at the machine console (not telnet/rsh, etc), this is safe.

## OPTIONS

### GLOBAL OPTIONS

This can be used for auth and account module types.

onerr=[fail|succeed]

If something weird happens (like unable to open the file), return with PAM\_SUCCESS if onerr=succeed is given, else with the corresponding PAM error code.

file=/path/to/counter

File where to keep counts. Default is /var/log/faillog.

audit

Will log the user name into the system log if the user is not found.

silent

Don't print informative messages.

no\_log\_info

Don't log informative messages via syslog(3).

### AUTH OPTIONS

Authentication phase first checks if user should be denied access and if not it increments attempted login counter. Then on call to pam\_setcred(3) it resets the attempts counter.

deny=n

Deny access if tally for this user exceeds n.

lock\_time=n

Always deny for n seconds after failed attempt.

unlock\_time=n

Allow access after n seconds after failed attempt. If this option is used the user will be locked out for the specified amount of time after he exceeded his maximum allowed attempts. Otherwise the account is locked until the lock is removed by a manual intervention of the system administrator.

magic\_root

If the module is invoked by a user with uid=0 the counter is not incremented. The sysadmin should use this for user launched services, like su, otherwise this argument should be omitted.

no\_lock\_time

Do not use the .fail\_locktime field in /var/log/faillog for this user.

no\_reset

Don't reset count on successful entry, only decrement.

even\_deny\_root\_account

Root account can become unavailable.

per\_user

If /var/log/faillog contains a non-zero .fail\_max/.fail\_locktime field for this user then use it instead of deny=n/ lock\_time=n parameter.

no\_lock\_time

Don't use .fail\_locktime field in /var/log/faillog for this user.

## ACCOUNT OPTIONS

Account phase resets attempts counter if the user is not magic root. This phase can be used optionally for services which don't call pam\_setcred(3) correctly or if the reset should be done regardless of the failure of the account phase of other modules.

magic\_root

If the module is invoked by a user with uid=0 the counter is not incremented. The sysadmin should use this for user launched services, like su, otherwise this argument should be omitted.

no\_reset

Don't reset count on successful entry, only decrement.

## MODULE TYPES PROVIDED

The auth and account module types are provided.

## RETURN VALUES

PAM\_AUTH\_ERR

A invalid option was given, the module was not able to retrieve the user name, no valid counter file was found, or too many failed logins.

PAM\_SUCCESS

Everything was successful.

## PAM\_USER\_UNKNOWN

User not known.

## EXAMPLES

Add the following line to `/etc/pam.d/login` to lock the account after too many failed logins. The number of allowed fails is specified by `/var/log/faillog` and needs to be set with `pam_tally` or `faillog(8)` before.

```
auth    required    pam_securetty.so
auth    required    pam_tally.so per_user
auth    required    pam_env.so
auth    required    pam_unix.so
auth    required    pam_nologin.so
account required    pam_unix.so
password required    pam_unix.so
session required    pam_limits.so
session required    pam_unix.so
session required    pam_lastlog.so nowtmp
session optional    pam_mail.so standard
```

## FILES

`/var/log/faillog`

failure logging file

## SEE ALSO

`faillog(8)`, `pam.conf(5)`, `pam.d(5)`, `pam(7)`

## AUTHOR

`pam_tally` was written by Tim Baverstock and Tomas Mraz.