NAME

pam_timestamp_check − Check to see if the default timestamp is valid

SYNOPSIS

pam_timestamp_check [−k] [−d] [*target_user*]

DESCRIPTION

With no arguments **pam_timestamp_check** will check to see if the default timestamp is valid, or optionally remove it.

OPTIONS

−k

Instead of checking the validity of a timestamp, remove it. This is analogous to sudo's *−k* option.

−d

Instead of returning validity using an exit status, loop indefinitely, polling regularly and printing the status on standard output.

target_user

By default **pam_timestamp_check** checks or removes timestamps generated by *pam_timestamp* when the user authenticates as herself. When the user authenticates as a different user, the name of the timestamp file changes to accommodate this. *target_user* allows to specify this user name.

RETURN VALUES

0

The timestamp is valid.

2

The binary is not setuid root.

3

Invalid invocation.

4

User is unknown.

5

Permissions error.

6

Invalid controlling tty.

7

Timestamp is not valid.

NOTES

Users can get confused when they are not always asked for passwords when running a given program. Some users reflexively begin typing information before noticing that it is not being asked for.

EXAMPLES

auth sufficient pam_timestamp.so verbose
auth required pam_unix.so

session required pam_unix.so
session optional pam_timestamp.so

FILES

/var/run/sudo/...

timestamp files and directories

SEE ALSO

pam_timestamp_check(8), **pam.conf**(5), **pam.d**(5), **pam**(7)

AUTHOR

pam_tally was written by Nalin Dahyabhai.