

NAME

`pam_loginuid` – Record user's login uid to the process attribute

SYNOPSIS

`pam_loginuid.so` [`require_auditd`]

DESCRIPTION

The `pam_loginuid` module sets the `loginuid` process attribute for the process that was authenticated. This is necessary for applications to be correctly audited. This PAM module should only be used for entry point applications like: `login`, `sshd`, `gdm`, `vsftpd`, `crond` and `atd`. There are probably other entry point applications besides these. You should not use it for applications like `sudo` or `su` as that defeats the purpose by changing the `loginuid` to the account they just switched to.

OPTIONS**`require_auditd`**

This option, when given, will cause this module to query the audit daemon status and deny logins if it is not running.

MODULE TYPES PROVIDED

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

RETURN VALUES**PAM_SUCCESS**

The `loginuid` value is set and `auditd` is running if check requested.

PAM_IGNORE

The `/proc/self/loginuid` file is not present on the system or the login process runs inside `uid` namespace and kernel does not support overwriting `loginuid`.

PAM_SESSION_ERR

Any other error prevented setting `loginuid` or `auditd` is not running.

EXAMPLES

```
##%PAM-1.0
auth    required  pam_unix.so
auth    required  pam_nologin.so
account required  pam_unix.so
password required pam_unix.so
session required  pam_unix.so
session required  pam_loginuid.so
```

SEE ALSO

`pam.conf(5)`, **`pam.d(5)`**, **`pam(7)`**, **`auditctl(8)`**, **`auditd(8)`**

AUTHOR

`pam_loginuid` was written by Steve Grubb <sgrubb@redhat.com>