

## NAME

`pam_lastlog` – PAM module to display date of last login and perform inactive account lock out

## SYNOPSIS

**pam\_lastlog.so** [`debug`] [`silent`] [`never`] [`nodate`] [`nohost`] [`noterm`] [`nowtmp`] [`noupdate`] [`showfailed`]  
[`inactive=<days>`] [`unlimited`]

## DESCRIPTION

`pam_lastlog` is a PAM module to display a line of information about the last login of the user. In addition, the module maintains the `/var/log/lastlog` file.

Some applications may perform this function themselves. In such cases, this module is not necessary.

The module checks **LASTLOG\_UID\_MAX** option in `/etc/login.defs` and does not update or display last login records for users with UID higher than its value. If the option is not present or its value is invalid, no user ID limit is applied.

If the module is called in the `auth` or `account` phase, the accounts that were not used recently enough will be disallowed to log in. The check is not performed for the root account so the root is never locked out. It is also not performed for users with UID higher than the **LASTLOG\_UID\_MAX** value.

## OPTIONS

### **debug**

Print debug information.

### **silent**

Don't inform the user about any previous login, just update the `/var/log/lastlog` file. This option does not affect display of bad login attempts.

### **never**

If the `/var/log/lastlog` file does not contain any old entries for the user, indicate that the user has never previously logged in with a welcome message.

### **nodate**

Don't display the date of the last login.

### **noterm**

Don't display the terminal name on which the last login was attempted.

### **nohost**

Don't indicate from which host the last login was attempted.

### **nowtmp**

Don't update the `wtmp` entry.

### **noupdate**

Don't update any file.

### **showfailed**

Display number of failed login attempts and the date of the last failed attempt from `btmp`. The date is not displayed when **nodate** is specified.

### **inactive=<days>**

This option is specific for the `auth` or `account` phase. It specifies the number of days after the last login of the user when the user will be locked out by the module. The default value is 90.

### **unlimited**

If the *fsize* limit is set, this option can be used to override it, preventing failures on systems with large UID values that lead `lastlog` to become a huge sparse file.

## MODULE TYPES PROVIDED

The **auth** and **account** module type allows one to lock out users who did not login recently enough. The **session** module type is provided for displaying the information about the last login and/or updating the `lastlog` and `wtmp` files.

**RETURN VALUES****PAM\_SUCCESS**

Everything was successful.

**PAM\_SERVICE\_ERR**

Internal service module error.

**PAM\_USER\_UNKNOWN**

User not known.

**PAM\_AUTH\_ERR**

User locked out in the auth or account phase due to inactivity.

**PAM\_IGNORE**

There was an error during reading the lastlog file in the auth or account phase and thus inactivity of the user cannot be determined.

**EXAMPLES**

Add the following line to `/etc/pam.d/login` to display the last login time of an user:

```
session required pam_lastlog.so nowtmp
```

To reject the user if he did not login during the previous 50 days the following line can be used:

```
auth required pam_lastlog.so inactive=50
```

**FILES**

`/var/log/lastlog`

Lastlog logging file

**SEE ALSO**

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

**AUTHOR**

`pam_lastlog` was written by Andrew G. Morgan <morgan@kernel.org>.

Inactive account lock out added by Tomáš Mráz <tm@t8m.info>.