

How to display password policy information for a user (Ubuntu)?

Published: 2010-06-09 · Archived: 2026-04-06 00:28:14 UTC

The OP confuses two different questions: *policy* and *password length*.

As already stated by @BillThor, password length is dealt with by the PAM module, under the not truly auspicious keyword `obscure`, in the file `/etc/pam.d/common-password`, which contains the following line:

```
password [success=1 default=ignore] pam_unix.so obscure sha512
```

The `obscure` keyword stands for (according to *man pam_unix*):

obscure

Enable some extra checks on password strength. These checks are based on the "obscure" checks in the original shadow package. The behavior is similar to the `pam_cracklib` module, but for non-dictionary-based checks. The following checks are implemented:

Palindrome

Verifies that the new password is not a palindrome of (i.e., the reverse of) the previous one.

Case Change Only

Verifies that the new password isn't the same as the old one with a change of case.

Similar

Verifies that the new password isn't too much like the previous one.

Simple

Is the new password too simple? This is based on the length of the password and the number of different types of characters (alpha, numeric, etc.) used.

Rotated

Is the new password a rotated version of the old password? (E.g., "billy" and "illyb")

The prescription by `obscure` can be overridden as follows: in `/etc/pam.d/common-password`, re-write the line above as

```
password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=20
```

or whatever you like.

Finding exactly where the minimum length password is defined requires diving into the depths of pam:

```
# apt-cache search pam_unix.so
libpam-modules - Pluggable Authentication Modules for PAM
# apt-get source libpam-modules
```

... and then to find where the minimum password length is defined:

```
# grep -rI UNIX_MIN_PASS_LEN
modules/pam_unix/support.h
modules/pam_unix/support.c
debian/patches-applied/007_modules_pam_unix
debian/patches-applied/055_pam_unix_nullok_secure
```

Perusing the debian patches you will see that the parameter `UNIX_MIN_PASS_LEN` (the 27th possible parameter) corresponds to a variable called **minlen**, which is set in `/modules/pam_unix/support.c`. However, one of the debian patches fixes `pass_min_len`: the file `debian/patches-applied/007_modules_pam_unix` contains the lines:

```
-     int pass_min_len = 0;
+     int pass_min_len = 6;
```

and the file `debian/Changelog` specifies:

- Further cleanups of `007_modules_pam_unix` -- don't use a global variable for `pass_min_len`, don't gratuitously move the length checking into the "obscure" checks, and internationalize the error strings.

I always disliked PAM, and for this reason: to locate a trivial parameter like the minimum password length, it obliges you to look into the source code.

The information displayed by `chage -l username` is instead completely contained in the `/etc/shadow` file: The [Man page](#) states:

```
shadow is a file which contains the password information for the system's accounts and optional aging information.
```

The fields of each entry are:

```
Login name, encrypted password, date of last password change, minimum password age, maximum password age, password warning period, password inactivity period, account expiration date, plus a reserved field for future use.
```

Just to double check, an `strace` of the `chage` command shows which files are opened,

```
# strace -e trace=open -f chage -l myusername
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
```

```
open("/lib/x86_64-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
open("/lib/x86_64-linux-gnu/libpcre.so.3", O_RDONLY|O_CLOEXEC) = 3
open("/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
open("/proc/filesystems", O_RDONLY) = 3
open("/usr/lib/locale/locale-archive", O_RDONLY|O_CLOEXEC) = 3
open("/etc/passwd", O_RDONLY|O_NOCTTY|O_NONBLOCK|O_NOFOLLOW) = 3
open("/etc/shadow", O_RDONLY|O_NOCTTY|O_NONBLOCK|O_NOFOLLOW) = 4
open("/usr/share/locale/locale.alias", O_RDONLY|O_CLOEXEC) = 5
open("/usr/share/locale/en_US/LC_MESSAGES/shadow.mo", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/usr/share/locale/en/LC_MESSAGES/shadow.mo", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/usr/share/locale-langpack/en_US/LC_MESSAGES/shadow.mo", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/usr/share/locale-langpack/en/LC_MESSAGES/shadow.mo", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/etc/localtime", O_RDONLY|O_CLOEXEC) = 5
Last password change          : mag 05, 2014
Password expires              : never
Password inactive             : never
Account expires               : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
+++ exited with 0 +++
```

Source: <https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu>