



Linux Ubuntu 26.04 Manual Pages on command 'passwd.1'

\$ man passwd.1

PASSWD(1) User Commands PASSWD(1)

NAME

passwd - change user password

SYNOPSIS

passwd [options] [LOGIN]

DESCRIPTION

The passwd command changes passwords for user accounts. A normal user may only change the password for their own account, while the superuser may change the password for any account.

passwd also changes the account or associated password validity period.

Password Changes

The user is first prompted for their old password, if one is present. This password is then encrypted and compared against the stored password. The user has only one chance to enter the correct password. The superuser is permitted to bypass this step so that forgotten passwords may be changed.

After the password has been entered, password aging information is checked to see if the user is permitted to change the password at this time. If not, passwd refuses to change the password and exits.

The user is then prompted twice for a replacement password. The second entry is compared against the first and both are required to match in order for the password to be changed.

Then, the password is tested for complexity. passwd will reject any password which is not suitably complex. Care must be taken not to include the system default erase or kill characters.

Hints for user passwords

The security of a password depends upon the strength of the encryption algorithm and the size of the key space. The legacy UNIX System encryption method is based on the NBS DES algorithm. More recent methods are now recommended (see ENCRYPT_METHOD). The size of the key space depends upon the randomness of the password which is selected.

Compromises in password security normally result from careless password selection or handling. For this reason, you should not select a password which appears in a dictionary or which must be written down. The password should also not be a proper name, your license number, birth date, or street address. Any of these may be used as guesses to violate system security.

As a general guideline, passwords should be long and random. It's fine to use simple character sets, such as passwords consisting only of lowercase letters, if that helps memorizing longer passwords. For a password consisting only of lowercase English letters randomly chosen, and a length of 32, there are 26^{32} (approximately 2^{150}) different possible combinations. Being an exponential equation, it's apparent that the exponent (the length) is more important than the base (the size of the character set).

You can find advice on how to choose a strong password on https://en.wikipedia.org/wiki/Password_strength

OPTIONS

The options which apply to the passwd command are:

-a, --all

This option can be used only with -S and causes show status for all users.

-d, --delete

Delete a user's password (make it empty). This is a quick way to disable a password for an account. It will set the named account passwordless.

-e, --expire

Immediately expire an account's password. This in effect can force a user to change their password at the user's next login.

-h, --help

Display help message and exit.

-i, --inactive INACTIVE

This option is used to disable an account after the password has been expired for a number of days. After a user account has had an expired password for INACTIVE days, the user may no longer sign on to the account.

-k, --keep-tokens

Indicate password change should be performed only for expired authentication tokens (passwords). The user wishes to keep their non-expired tokens as before.

-l, --lock

Lock the password of the named account. This option disables a password by changing it to a value which matches no possible encrypted value (it adds a `?!?` at the beginning of the password).

Note that this does not disable the account. The user may still be able to login using another authentication token (e.g. an SSH key). To disable the account, administrators should use `usermod --expiredate 1` (this sets the account's expire date to Jan 2, 1970).

Users with a locked password are not allowed to change their password.

-n, --mindays MIN_DAYS

Set the minimum number of days between password changes to `MIN_DAYS`. A value of zero for this field indicates that the user may change their password at any time.

-q, --quiet

Quiet mode.

-r, --repository REPOSITORY

change password in `REPOSITORY` repository

-R, --root CHROOT_DIR

Apply changes in the `CHROOT_DIR` directory and use the configuration files from the `CHROOT_DIR` directory. Only absolute paths are supported.

-P, --prefix PREFIX_DIR

Apply changes to configuration files under the root filesystem found under the directory `PREFIX_DIR`. This option does not chroot and is intended for preparing a cross-compilation target. Some limitations: NIS and LDAP users/groups are not verified.

No PAM support. No SELINUX support.

-S, --status

Display account status information. The status information consists of 7 fields. The first field is the user's login name. The second field indicates if the user account has a locked password (L), has no password (NP), or has a usable password (P). The third field gives the date of the last password change. The next four fields are the minimum age, maximum age, warning period, and inactivity period for the password. These ages are expressed in days.

`-u, --unlock`

Unlock the password of the named account. This option re-enables a password by changing the password back to its previous value (to the value before using the `-l` option).

`-w, --warndays WARN_DAYS`

Set the number of days of warning before a password change is required. The `WARN_DAYS` option is the number of days prior to the password expiring that a user will be warned that their password is about to expire.

`-x, --maxdays MAX_DAYS`

Set the maximum number of days a password remains valid. After `MAX_DAYS`, the password is required to be changed.

Passing the number `-1` as `MAX_DAYS` will remove checking a password's validity.

`-s, --stdin`

This option is used to indicate that `passwd` should read the new password from standard input, which can be a pipe.

CAVEATS

Password complexity checking may vary from site to site. The user is urged to select a password as complex as he or she feels comfortable with.

Users may not be able to change their password on a system if NIS is enabled and they are not logged into the NIS server.

`passwd` uses PAM to authenticate users and to change their passwords.

FILES

`/etc/passwd`

User account information.

`/etc/shadow`

Secure user account information.

`/etc/pam.d/passwd`

PAM configuration for `passwd`.

EXIT VALUES

The `passwd` command exits with the following values:

0

success

1

permission denied

2

invalid combination of options

3

unexpected failure, nothing done

4

unexpected failure, passwd file missing

5

passwd file busy, try again

6

invalid argument to option

SEE ALSO

chpasswd(8), makepasswd(1), passwd(5), shadow(5), usermod(8).

The following web page comically (yet correctly) compares the strength of two different methods for choosing a password: "<https://xkcd.com/936/>"

shadow-utils 4.17.4

02/02/2026

PASSWD(1)