Red Hat Enterprise Linux Release 9.2 Manual Pages on 'passwd.1' command

$ man passwd.1

```
PASSWD(1)                   User utilities                   PASSWD(1)

NAME

       passwd - update user's authentication tokens

SYNOPSIS

       passwd  [-k]  [-l]  [-u  [-f]]  [-d] [-e] [-n mindays] [-x maxdays] [-w

       warndays] [-i inactivedays] [-S] [--stdin] [-?] [--usage] [username]

DESCRIPTION

       The passwd utility is used to update user's authentication token(s).

       This task is achieved through calls to the Linux-PAM and  Libuser  API.

       Essentially, it initializes itself as a "passwd" service with Linux-PAM

       and utilizes configured password modules to authenticate and  then  up?

       date a user's password.

       A simple entry in the global Linux-PAM configuration file for this ser?

       vice would be:

        #

        # passwd service entry that does strength checking of

        # a proposed password before updating it.

        #

        passwd password requisite pam_cracklib.so retry=3

        passwd password required pam_unix.so use_authtok

        #

       Note, other module types are not required for this application to func?

       tion correctly.
```

OPTIONS

-k, --keep-tokens

The option -k is used to indicate that the update should only be for expired authentication tokens (passwords); the user wishes to keep their non-expired tokens as before.

-l, --lock

This option is used to lock the password of specified account and it is available to root only. The locking is performed by rendering the encrypted password into an invalid string (by pre? fixing the encrypted string with an !). Note that the account is not fully locked - the user can still log in by other means of authentication such as the ssh public key authentication. Use chage -E 0 user command instead for full account locking.

--stdin

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

-u, --unlock

This is the reverse of the -l option - it will unlock the ac? count password by removing the ! prefix. This option is avail? able to root only. By default passwd will refuse to create a passwordless account (it will not unlock an account that has only "!" as a password). The force option -f will override this protection.

-d, --delete

This is a quick way to delete a password for an account. It will set the named account passwordless. Available to root only. Note that if the password was locked, this implicitly removes the password lock as well.

-e, --expire

This is a quick way to expire a password for an account. The user will be forced to change the password during the next login attempt. Available to root only.

-f, --force

Force the specified operation.

-n, --minimum DAYS

This will set the minimum password lifetime, in days, if the user's account supports password lifetimes. Available to root only.

-x, --maximum DAYS

This will set the maximum password lifetime, in days, if the user's account supports password lifetimes. Available to root only.

-w, --warning DAYS

This will set the number of days in advance the user will begin receiving warnings that her password will expire, if the user's account supports password lifetimes. Available to root only.

-i, --inactive DAYS

This will set the number of days which will pass before an ex? pired password for this account will be taken to mean that the account is inactive and should be disabled, if the user's ac? count supports password lifetimes. Available to root only.

-S, --status

This will output a short information about the status of the password for a given account. 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 (LK), has no password (NP), or has a usable password (PS). The third field gives the date of the last password change. The next four fields are the minimum age, maximum age, warning period, and in? activity period for the password. These ages are expressed in days.

Notes: The date of the last password change is stored as a num? ber of days since epoch. Depending on the current time zone, the passwd -S username may show the date of the last password change that is different from the real date of the last password change by ?1 day.

This option is available to root only.

-?, --help

Print a help message and exit.

--usage

Print a short usage message and exit.

Remember the following two principles

Protect your password.

Don't write down your password - memorize it. In particular, don't write it down and leave it anywhere, and don't place it in an unencrypted file! Use unrelated passwords for systems con? trolled by different organizations. Don't give or share your password, in particular to someone claiming to be from computer support or a vendor. Don't let anyone watch you enter your password. Don't enter your password to a computer you don't trust or if things "look funny"; someone may be trying to hijack your password. Use the password for a limited time and change it periodically.

Choose a hard-to-guess password.

passwd through the calls to the pam_cracklib PAM module will try to prevent you from choosing a really bad password, but it isn't foolproof; create your password wisely. Don't use something you'd find in a dictionary (in any language or jargon). Don't use a name (including that of a spouse, parent, child, pet, fan? tasy character, famous person, and location) or any variation of your personal or account name. Don't use accessible information about you (such as your phone number, license plate, or social security number) or your environment. Don't use a birthday or a simple pattern (such as "qwerty", "abc", or "aaa"). Don't use any of those backwards, followed by a digit, or preceded by a digit. Instead, use a mixture of upper and lower case letters, as well as digits or punctuation. When choosing a new password, make sure it's unrelated to any previous password. Use long passwords (say at least 8 characters long). You might use a

word pair with punctuation inserted, a passphrase (an under?
standable sequence of words), or the first letter of each word
in a passphrase.

These principles are partially enforced by the system, but only partly so. Vigilance on your part will make the system much more secure.

EXIT CODE

The passwd command exits with the following codes:

0

success

1

passwd/libuser operation failed

2

unknown user

252

unknown user name

253

bad arguments or passwordless account

254

invalid application of arguments

255

libuser operation failed

Error messages are written to the standard error stream.

CONFORMING TO

Linux-PAM (Pluggable Authentication modules for Linux).

FILES

/etc/pam.d/passwd - the Linux-PAM configuration file

BUGS

None known.

SEE ALSO

pam(8), pam.d(5), libuser.conf(5), and pam_chauthtok(3).

For more complete information on how to configure this application with Linux-PAM, see the Linux-PAM System Administrators' Guide.

AUTHOR

Cristian Gafton <gafton@redhat.com>

GNU/Linux Mar 28 2018 PASSWD(1)