NAME

passwd – change login password and password attributes

SYNOPSIS

passwd [*name*]

passwd –r files [**–egh**] [*name*]

passwd –r files –s [**–a**]

passwd –r files –s [*name*]

passwd –r files [**–d** | **–l**] [**–f**] [**–n** *min*] [**–w** *warn*] [**–x** *max*] *name*

passwd –r nis [**–egh**] [*name*]

passwd –r nisplus [**–egh**] [**–D** *domainname*] [*name*]

passwd –r nisplus –s [**–a**]

passwd –r nisplus [**–D** *domainname*] **–s** [*name*]

passwd –r nisplus [**–l**] [**–f**] [**–n** *min*] [**–w** *warn*] [**–x** *max*] [**–D** *domainname*] *name*

AVAILABILITY

SUNWcsu

DESCRIPTION

The **passwd** command changes the password or lists password attributes associated with the user's login *name*. Additionally, privileged users may use **passwd** to install or change passwords and attributes associated with any login *name*.

When used to change a password, **passwd** prompts everyone for their old password, if any. It then prompts for the new password twice. When the old password is entered, **passwd** checks to see if it has "aged" sufficiently. If "aging" is insufficient, **passwd** terminates; see **pwconv**(1M), **nistbladm**(1), and **shadow**(4) for additional information. The **pwconv** command creates and updates **/etc/shadow** with information from **/etc/passwd**. **pwconv** relies on a special value of 'x' in the password field of **/etc/passwd**. This value of 'x' indicates that the password for the user is already in **/etc/shadow** and should not be modified.

If aging is sufficient, a check is made to ensure that the new password meets construction requirements. When the new password is entered a second time, the two copies of the new password are compared. If the two copies are not identical the cycle of prompting for the new password is repeated for at most two more times.

Passwords must be constructed to meet the following requirements:

- Each password must have at least six characters. Only the first eight characters are significant. **PASSLENGTH** is found in **/etc/default/passwd** and is set to **6**.
- Each password must contain at least two alphabetic characters and at least one numeric or special character. In this case, "alphabetic" refers to all upper or lower case letters.
- Each password must differ from the user's login *name* and any reverse or circular shift of that login *name*. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent.

- New passwords must differ from the old by at least three characters. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent.

If all requirements are met, by default, the **passwd** command will consult **/etc/nsswitch.conf** to determine in which repositories to perform password update. It searches the **passwd** and **passwd_compat** entries. The sources (repositories) associated with these entries will be updated. However, the password update configurations supported are limited to the following 5 cases. Failure to comply with the configurations will prevent users from logging onto the system.

- **passwd: files**
- **passwd: files nis**
- **passwd: files nisplus**
- **passwd: compat** (==> files nis)
- **passwd: compat** (==> files nisplus)
  passwd_compat: nisplus

Network administrators, who own the NIS+ password table, may change any password attributes.

In **files** case, super-users (for instance, real and effective uid equal to zero, see **id**(1M) and **su**(1M)) may change any password; hence, **passwd** does not prompt privileged users for the old password. Privileged users are not forced to comply with password aging and password construction requirements. A privileged user can create a null password by entering a carriage return in response to the prompt for a new password. (This differs from **passwd** −**d** because the "password" prompt will still be displayed.)

Any user may use the −**s** option to show password attributes for his or her own login *name*. Provided they are using the −**r nisplus** argument. Otherwise the −**s** argument is restricted to the super-user.

The format of the display will be:

name status mm/dd/yy min max warn

or, if password aging information is not present,

name status

where

name The login ID of the user.

status The password status of *name*: **PS** stands for passworded or locked, **LK** stands for locked, and **NP** stands for no password.

mm/dd/yy
The date password was last changed for *name*. (Note that all password aging dates are determined using Greenwich Mean Time (Universal Time) and, therefore, may differ by as much as a day in other time zones.)

min The minimum number of days required between password changes for *name*. **MINWEEKS** is found in **/etc/default/passwd** and is set to **NULL**.

max The maximum number of days the password is valid for *name*. **MAXWEEKS** is found in **/etc/default/passwd** and is set to **NULL**.

warn The number of days relative to *max* before the password expires and the *name* will be warned.

OPTIONS

–r Specifies the repository to which an operation is applied. The supported repositories are **files**, **nis**, or **nisplus**.

–e Change the login shell.

–g Change the gecos (finger) information.

–h Change the home directory.

–D *domainname* Consult the **passwd.org_dir** table in *domainname*. If this option is not specified, the default *domainname* returned by **nis_local_directory**(3N) will be used. This domain name is the same as that returned by **domainname**(1M).

–s *name* Show password attributes for the login *name*. For the **nisplus** repository, this works for everyone. However for the **files** repository, this only works for the super-user. It does not work at all for the **nis** repository which does not support password aging.

–a Show password attributes for all entries. Use only with the **–s** option; *name* must not be provided. For **nisplus** repository, this will show only the entries in the NIS+ passwd table in the local domain that the invoker is authorized to "read". For the **files** repository, this is restricted to the super-user.

Privileged User Options

Only a privileged user can use the following options:

–f Force the user to change password at the next login by expiring the password for *name*.

–l Locks password entry for *name*.

–n *min* Set minimum field for *name*. The *min* field contains the minimum number of days between password changes for *name*. If *min* is greater than *max*, the user may not change the password. Always use this option with the **–x** option, unless *max* is set to **–1** (aging turned off). In that case, *min* need not be set.

–w *warn* Set warn field for *name*. The *warn* field contains the number of days before the password expires and the user is warned.

–x *max* Set maximum field for *name*. The *max* field contains the number of days that the password is valid for *name*. The aging for *name* will be turned off immediately if *max* is set to **–1**. If it is set to **0**, then the user is forced to change the password at the next login session and aging is turned off.

–d Deletes password for *name*. The login *name* will not be prompted for password. It is only applicable to the **files** repository.

ENVIRONMENT

If any of the **LC_∗** variables (**LC_CTYPE, LC_MESSAGES, LC_TIME, LC_COLLATE, LC_NUMERIC,** and **LC_MONETARY**) (see **environ**(5)) are not set in the environment, the operational behavior of **passwd** for each corresponding locale category is determined by the value of the **LANG** environment variable. If **LC_ALL** is set, its contents are used to override both the **LANG** and the other **LC_∗** variables. If none of the above variables is set in the environment, the "C" (U.S. style) locale determines how **passwd** behaves.

LC_CTYPE Determines how **passwd** handles characters. When **LC_CTYPE** is set to a valid value, **passwd** can display and handle text and filenames containing valid characters for that locale. **passwd** can display and handle Extended Unix Code (EUC) characters where any individual character can be 1, 2, or 3 bytes wide. **passwd** can also handle EUC characters of 1, 2, or more column widths. In the "C" locale, only characters from ISO 8859-1 are valid.

LC_MESSAGES Determines how diagnostic and informative messages are presented. This includes the language and style of the messages, and the correct form of affirmative and negative responses. In the "C" locale, the messages are presented in the default form found in the program itself (in most cases, U.S. English).

EXIT STATUS

The **passwd** command exits with one of the following values:

0 success.
1 Permission denied.
2 Invalid combination of options.
3 Unexpected failure. Password file unchanged.
4 Unexpected failure. Password file(s) missing.
5 Password file(s) busy. Try again later.
6 Invalid argument to option.

FILES

/etc/oshadow
/etc/passwd password file.
/etc/shadow shadow password file.
/etc/default/passwd Default values can be set for the following flags in **/etc/default/passwd**. For example: **MAXWEEKS=26**

MAXWEEKS Maximum time period that password is valid.

MINWEEKS Minimum time period before the password can be changed.

PASSLENGTH Minimum length of password, in characters.

WARNWEEKS Time period until warning of date of password's ensuing expiration.

SEE ALSO

finger(1), **login**(1), **nispasswd**(1), **yppasswd**(1), **domainname**(1M), **eeprom**(1M), **id**(1M), **passmgmt**(1M), **pwconv**(1M), **su**(1M), **useradd**(1M), **userdel**(1M), **usermod**(1M), **crypt**(3C), **getpwnam**(3C), **getspnam**(3C), **nis_local_directory**(3N), **loginlog**(4), **passwd**(4), **shadow**(4), **environ**(5)

NOTES

The **passwd** command replaces the **nispasswd** and **yppasswd** commands and should be used in their place.