NAME

nispasswd – change NIS+ password information

SYNOPSIS

nispasswd [**–ghs**] [**–D** *domainname*] [*username*]

nispasswd –a

nispasswd –**D** *domainname* [–**d** [*username*]]

nispasswd [**–l**] [**–f**] [**–n** *min*] [**–x** *max*] [**–w** *warn*] [**–D** *domainname*] *username*

AVAILABILITY

SUNWnisu

DESCRIPTION

nispasswd changes a password, gecos (finger) field (**–g** option), home directory (**–h** option), or login shell (**–s** option) associated with the *username* (invoker by default) in the NIS+ passwd table.

Additionally, the command can be used to view or modify aging information associated with the user specified if the invoker has the right NIS+ privileges.

nispasswd uses secure RPC to communicate with the NIS+ server, and therefore, never sends unencrypted passwords over the communication medium.

nispasswd does not read or modify the local password information stored in the **/etc/passwd** and **/etc/shadow** files.

When used to change a password, **nispasswd** prompts non-privileged users for their old password. It then prompts for the new password twice to forestall typing mistakes. When the old password is entered, **nispasswd** checks to see if it has “aged” sufficiently. If “aging” is insufficient, **nispasswd** terminates; see **getspnam**(3C).

The old password is used to decrypt the username’s secret key. If the password does not decrypt the secret key, **nispasswd** prompts for the old secure-RPC password. It uses this password to decrypt the secret key. If this fails, it gives the user one more chance. The old password is also used to ensure that the new password differs from the old by at least three characters. Assuming aging is sufficient, a check is made to ensure that the new password meets construction requirements described below. 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 twice. The new password is used to re-encrypt the user’s secret key. Hence, it also becomes their secure-RPC password. Therefore, the secure-RPC is no longer a different password from the user’s password.

Passwords must be constructed to meet the following requirements:

- Each password must have at least six characters. Only the first eight characters are significant.
- 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 *username* and any reverse or circular shift of that login *username*. 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.

Network administrators, who own the NIS+ password table, may change any password attributes if they establish their credentials (see **keylogin**(1)) before invoking **nispasswd**. Hence, **nispasswd** does not prompt these privileged-users for the old password and they are not forced to comply with password aging and password construction requirements.

Any user may use the −**d** option to display password attributes for his or her own login name. The format of the display will be:

username status mm/dd/yy min max warn

or, if password aging information is not present,

username status

where

username	The login ID of the user.
status	The password status of *username*: "PS" stands for password exists or locked, "LK" stands for locked, and "NP" stands for no password.
mm/dd/yy	The date password was last changed for *username*. (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 *username*.
max	The maximum number of days the password is valid for *username*.
warn	The number of days relative to *max* before the password expires that the *username* will be warned.

OPTIONS

−**g**	Change the gecos (finger) information.
−**h**	Change the home directory.
−**s**	Change the login shell. By default, only the NIS+ administrator can change the login shell. User will be prompted for the new login shell.
−**a**	Show the password attributes for all entries. This will show only the entries in the NIS+ passwd table in the local domain that the invoker is authorized to "read".
−**d** [*username*]	Display password attributes for the caller or the user specified if the invoker has the right privileges.
−**l**	Locks the password entry for *username*. Subsequently, **login**(1) would disallow logins with this NIS+ password entry.
−**f**	Force the user to change password at the next login by expiring the

password for *username*.

–n *min* Set minimum field for *username*. The *min* field contains the minimum number of days between password changes for *username*. 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.

–x *max* Set maximum field for *username*. The *max* field contains the number of days that the password is valid for *username*. The aging for *username* 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.

–w *warn* Set *warn* field for *username*. The *warn* field contains the number of days before the password expires that the user will be warned whenever he or she attempts to login.

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

EXIT STATUS

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

0 success.
1 Permission denied.
2 Invalid combination of options.
3 Unexpected failure. NIS+ passwd table unchanged.
4 NIS+ passwd table missing.
5 NIS+ is busy. Try again later.
6 Invalid argument to option.
7 Aging is disabled.

SEE ALSO

keylogin(1), **login**(1), **nis+**(1), **nistbladm**(1), **passwd**(1), **domainname**(1M), **getspnam**(3C), **getpwnam**(3C), **nsswitch.conf**(4), **passwd**(4), **shadow**(4)

NOTES

The use of **nispasswd** is discouraged, as it is now only a link to the **passwd**(1) command, which should be used instead. Using **passwd**(1) with the **–r nisplus** option will achieve the same result, and be consistent across all the different name services available.

The login program, file access display programs (for example, '**ls –l**') and network programs that require user passwords (for example, **rlogin**(1), **ftp**(1), etc.) use the standard **getpwnam**(3C) and **getspnam**(3C) interfaces to get password information. These programs will get the NIS+ password information, that is modified by **nispasswd**, only if the **passwd:** entry in the **/etc/nsswitch.conf** file includes **nisplus**. See **nsswitch.conf**(4) for more details.