

NAME

chpasswd – update passwords in batch mode

SYNOPSIS

chpasswd [*options*]

DESCRIPTION

The **chpasswd** command reads a list of user name and password pairs from standard input and uses this information to update a group of existing users. Each line is of the format:

user_name:password

By default the passwords must be supplied in clear-text, and are encrypted by **chpasswd**. Also the password age will be updated, if present.

By default, passwords are encrypted by PAM, but (even if not recommended) you can select a different encryption method with the **-e**, **-m**, or **-c** options.

Except when PAM is used to encrypt the passwords, **chpasswd** first updates all the passwords in memory, and then commits all the changes to disk if no errors occurred for any user.

When PAM is used to encrypt the passwords (and update the passwords in the system database) then if a password cannot be updated **chpasswd** continues updating the passwords of the next users, and will return an error code on exit.

This command is intended to be used in a large system environment where many accounts are created at a single time.

OPTIONS

The options which apply to the **chpasswd** command are:

-c, --crypt-method METHOD

Use the specified method to encrypt the passwords.

The available methods are DES, MD5, NONE, and SHA256 or SHA512 if your libc support these methods.

By default, PAM is used to encrypt the passwords.

-e, --encrypted

Supplied passwords are in encrypted form.

-h, --help

Display help message and exit.

-m, --md5

Use MD5 encryption instead of DES when the supplied passwords are not encrypted.

-R, --root CHROOT_DIR

Apply changes in the *CHROOT_DIR* directory and use the configuration files from the *CHROOT_DIR* directory.

-s, --sha-rounds ROUNDS

Use the specified number of rounds to encrypt the passwords.

The value 0 means that the system will choose the default number of rounds for the crypt method (5000).

A minimal value of 1000 and a maximal value of 999,999,999 will be enforced.

You can only use this option with the SHA256 or SHA512 crypt method.

By default, the number of rounds is defined by the **SHA_CRYPT_MIN_ROUNDS** and

SHA_CRYPT_MAX_ROUNDS variables in `/etc/login.defs`.

CAVEATS

Remember to set permissions or umask to prevent readability of unencrypted files by other users.

CONFIGURATION

The following configuration variables in `/etc/login.defs` change the behavior of this tool:

SHA_CRYPT_MIN_ROUNDS (number), **SHA_CRYPT_MAX_ROUNDS** (number)

When **ENCRYPT_METHOD** is set to *SHA256* or *SHA512*, this defines the number of SHA rounds used by the encryption algorithm by default (when the number of rounds is not specified on the command line).

With a lot of rounds, it is more difficult to brute forcing the password. But note also that more CPU resources will be needed to authenticate users.

If not specified, the libc will choose the default number of rounds (5000).

The values must be inside the 1000–999,999,999 range.

If only one of the **SHA_CRYPT_MIN_ROUNDS** or **SHA_CRYPT_MAX_ROUNDS** values is set, then this value will be used.

If **SHA_CRYPT_MIN_ROUNDS** > **SHA_CRYPT_MAX_ROUNDS**, the highest value will be used.

Note: This only affect the generation of group passwords. The generation of user passwords is done by PAM and subject to the PAM configuration. It is recommended to set this variable consistently with the PAM configuration.

FILES

`/etc/passwd`

User account information.

`/etc/shadow`

Secure user account information.

`/etc/login.defs`

Shadow password suite configuration.

`/etc/pam.d/chpasswd`

PAM configuration for **chpasswd**.

SEE ALSO

passwd(1), **newusers**(8), **login.defs**(5), **useradd**(8).