Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'chpasswd.8' command

$ man chpasswd.8

```
CHPASSWD(8)          System Management Commands          CHPASSWD(8)

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.

       The default encryption algorithm can be defined for the system with the

       ENCRYPT_METHOD or MD5_CRYPT_ENAB variables of /etc/login.defs, and can

       be overwritten with the -e, -m, or -c options.

       chpasswd first updates all the passwords in memory, and then commits

       all the changes to disk if no errors occurred for any user.

       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 (if none of the -c, -m, or -e options are specified), the encryption method is defined by the ENCRYPT_METHOD or MD5_CRYPT_ENAB variables of /etc/login.defs.

-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:

ENCRYPT_METHOD (string)

This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line).

It can take one of these values: DES (default), MD5, SHA256, SHA512. MD5 and DES should not be used for new hashes, see crypt(5) for recommendations.

Note: this parameter overrides the MD5_CRYPT_ENAB variable.

MD5_CRYPT_ENAB (boolean)

Indicate if passwords must be encrypted using the MD5-based algorithm. If set to yes, new passwords will be encrypted using the MD5-based algorithm compatible with the one used by recent releases of FreeBSD. It supports passwords of unlimited length and longer salt strings. Set to no if you need to copy encrypted passwords to other systems which don't understand the new algorithm. Default is no.

This variable is superseded by the ENCRYPT_METHOD variable or by any command line option used to configure the encryption algorithm.

This variable is deprecated. You should use ENCRYPT_METHOD.

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), which is orders of magnitude too low for modern hardware.

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.

FILES

/etc/passwd

User account information.

/etc/shadow

Secure user account information.

/etc/login.defs

Shadow password suite configuration.

SEE ALSO

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