Rocky Enterprise Linux 9.2 Manual Pages on command 'systemd-ask-password.1'

$ man systemd-ask-password.1

SYSTEMD-ASK-PASSWORD(1)   systemd-ask-password   SYSTEMD-ASK-PASSWORD(1)

NAME

systemd-ask-password - Query the user for a system password

SYNOPSIS

systemd-ask-password [OPTIONS...] [MESSAGE]

DESCRIPTION

systemd-ask-password may be used to query a system password or passphrase from the user,

using a question message specified on the command line. When run from a TTY it will query

a password on the TTY and print it to standard output. When run with no TTY or with

--no-tty it will use the system-wide query mechanism, which allows active users to respond

via several agents, listed below.

The purpose of this tool is to query system-wide passwords ? that is passwords not

attached to a specific user account. Examples include: unlocking encrypted hard disks when

they are plugged in or at boot, entering an SSL certificate passphrase for web and VPN

servers.

Existing agents are:

?   A boot-time password agent asking the user for passwords using plymouth(8),

?   A boot-time password agent querying the user directly on the console ? systemd-ask-

password-console.service(8),

?   An agent requesting password input via a wall(1) message ? systemd-ask-password-

wall.service(8),

?   A TTY agent that is temporarily spawned during systemctl(1) invocations,

?   A command line agent which can be started temporarily to process queued password

requests ? systemd-tty-ask-password-agent --query.

Answering system-wide password queries is a privileged operation, hence all the agents listed above (except for the last one), run as privileged system services. The last one also needs elevated privileges, so should be run through sudo(8) or similar.

Additional password agents may be implemented according to the systemd Password Agent Specification[1].

If a password is queried on a TTY, the user may press TAB to hide the asterisks normally shown for each character typed. Pressing Backspace as first key achieves the same effect.

OPTIONS

The following options are understood:

--icon=

Specify an icon name alongside the password query, which may be used in all agents supporting graphical display. The icon name should follow the XDG Icon Naming Specification[2].

--id=

Specify an identifier for this password query. This identifier is freely choosable and allows recognition of queries by involved agents. It should include the subsystem doing the query and the specific object the query is done for. Example: "--id=cryptsetup:/dev/sda5".

--keyname=

Configure a kernel keyring key name to use as cache for the password. If set, then the tool will try to push any collected passwords into the kernel keyring of the root user, as a key of the specified name. If combined with --accept-cached, it will also try to retrieve such cached passwords from the key in the kernel keyring instead of querying the user right away. By using this option, the kernel keyring may be used as effective cache to avoid repeatedly asking users for passwords, if there are multiple objects that may be unlocked with the same password. The cached key will have a timeout of 2.5min set, after which it will be purged from the kernel keyring. Note that it is possible to cache multiple passwords under the same keyname, in which case they will be stored as NUL-separated list of passwords. Use keyctl(1) to access the cached key via the kernel keyring directly. Example: "--keyname=cryptsetup"

--credential=

Configure a credential to read the password from ? if it exists. This may be used in

conjunction with the LoadCredential= and SetCredential= settings in unit files. See
systemd.exec(5) for details. If not specified, defaults to "password". This option has
no effect if no credentials directory is passed to the program (i.e.
$CREDENTIALS_DIRECTORY is not set) or if the no credential of the specified name
exists.

--timeout=

Specify the query timeout in seconds. Defaults to 90s. A timeout of 0 waits
indefinitely.

--echo=yes|no|masked

Controls whether to echo user input. Takes a boolean or the special string "masked",
the default being the latter. If enabled the typed characters are echoed literally,
which is useful for prompting for usernames and other non-protected data. If disabled
the typed characters are not echoed in any form, the user will not get feedback on
their input. If set to "masked", an asterisk ("*") is echoed for each character typed.
In this mode, if the user hits the tabulator key ("?"), echo is turned off.
(Alternatively, if the user hits the backspace key ("?") while no data has been
entered otherwise, echo is turned off, too).

--echo, -e

Equivalent to --echo=yes, see above.

--emoji=yes|no|auto

Controls whether or not to prefix the query with a lock and key emoji (?), if the TTY
settings permit this. The default is "auto", which defaults to "yes", unless
--echo=yes is given.

--no-tty

Never ask for password on current TTY even if one is available. Always use agent
system.

--accept-cached

If passed, accept cached passwords, i.e. passwords previously entered.

--multiple

When used in conjunction with --accept-cached accept multiple passwords. This will
output one password per line.

--no-output

Do not print passwords to standard output. This is useful if you want to store a

password in kernel keyring with --keyname= but do not want it to show up on screen or in logs.

-n

By default, when writing the acquired password to standard output it is suffixed by a newline character. This may be turned off with the -n switch, similar to the switch of the same name of the echo(1) command.

-h, --help

Print a short help text and exit.

EXIT STATUS

On success, 0 is returned, a non-zero failure code otherwise.

SEE ALSO

systemd(1), systemd-ask-password-console.service(8), systemd-tty-ask-password-agent(1), keyctl(1), plymouth(8), wall(1)

NOTES

1. systemd Password Agent Specification

   https://systemd.io/PASSWORD_AGENTS/

2. XDG Icon Naming Specification

   http://standards.freedesktop.org/icon-naming-spec/icon-naming-spec-latest.html

systemd 249   SYSTEMD-ASK-PASSWORD(1)