NAME

cryptsetup-erase, cryptsetup-luksErase − erase all keyslots

SYNOPSIS

cryptsetup *erase* **[<options>] <device>**
cryptsetup *luksErase* **[<options>] <device>**

DESCRIPTION

Erase all keyslots, removing the volume key. Unless the device is configured with OPAL self−encrypting drive support, you do not need to provide any password for this operation.

This operation is irreversible. Unless you have a header backup, all old encrypted data in the container will be permanently irretrievable. Header backup cannot be used to recover data from OPAL self−encrypting drives, as the keys are permanently removed from hardware.

The **erase** does not wipe or overwrite the data area. It only removes all active keyslots from the LUKS device. See the cryptsetup FAQ for more information on how to wipe the whole device, including encrypted data.

Note that the −−hw−opal−factory−reset option for OPAL self−encrypting drive will erase ALL data on the drive, regardless of the partition it is run on.

<options> can be [−−header, −−disable−locks, −−hw−opal−factory−reset, −−key−file].

OPTIONS

−−batch−mode, **−q**
Suppresses all confirmation questions. Use with care!

If the −−verify−passphrase option is not specified, this option also switches off the passphrase verification.

−−debug or **−−debug−json**
Run in debug mode with full diagnostic logs. Debug output lines are always prefixed by #.

If −−debug−json is used, additional LUKS2 JSON data structures are printed.

−−disable−locks
Disable lock protection for metadata on disk. This option is valid only for LUKS2 and is ignored for other formats.

WARNING: Do not use this option unless you run cryptsetup in a restricted environment where locking is impossible to perform (where /run directory cannot be used).

−−header *<device or file storing the LUKS header>*
Use to specify a detached LUKS2 header when erasing OPAL self−encrypting drive.

−−help, **−?**
Show help text and default parameters.

−−hw−opal−factory−reset
Erase **ALL** data on the OPAL self−encrypting drive. The option does not require a valid LUKS2 header to be present on the device to run. After providing the correct PSID via interactive prompt or via −−key−file parameter the device is erased.

PSID is usually printed on the OPAL drive label (either directly or as a QR code). PSID must be entered without any dashes, spaces or underscores.

PSID should be treated as sensitive information as it allows anyone with remote access to the OPAL drive to destroy data even if the device is locked. Be sure you do not leak PSID through transparent packaging during transport or images of the drive posted online.

−−key−file, **−d** *file* (LUKS2 with HW OPAL only)
Read the Admin PIN or PSID (with −−hw−opal−factory−reset) from the file, depending on options used.

If the name given is "−", then the secret will be read from stdin. In this case, reading will not stop at newline characters.

−−usage
Show short option help.

−−version, **−V**
Show the program version.

REPORTING BUGS

Report bugs at cryptsetup mailing list <cryptsetup@lists.linux.dev> or in Issues project section <https://gitlab.com/cryptsetup/cryptsetup/−/issues/new>.

Please attach the output of the failed command with −−debug option added.

SEE ALSO

Cryptsetup FAQ <https://gitlab.com/cryptsetup/cryptsetup/wikis/FrequentlyAskedQuestions>

cryptsetup(8), **integritysetup**(8) and **veritysetup**(8)

CRYPTSETUP

Part of cryptsetup project <https://gitlab.com/cryptsetup/cryptsetup/>.