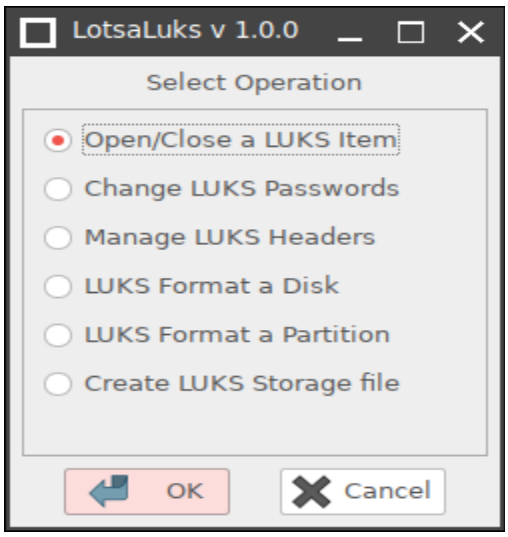
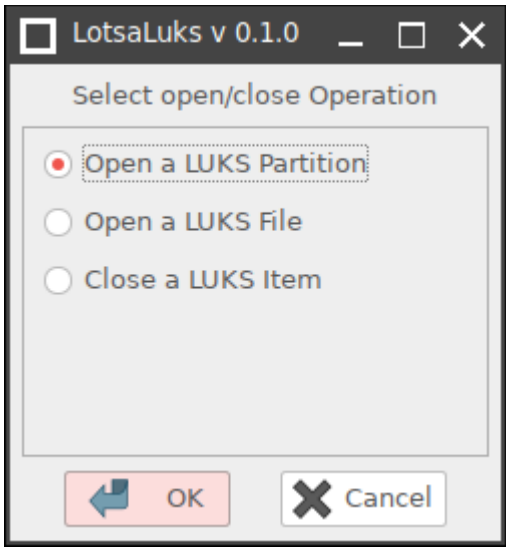
LotsaLuks File/Disk Encryption Tool for Puppy Linux



LotsaLuks v1.0.0 is a GUI frontend for the ‘cryptsetup/LUKS’ suite of encryption tools. It is intended to simplify the process of creating and managing LUKS disks, partitions, files, and passwords.

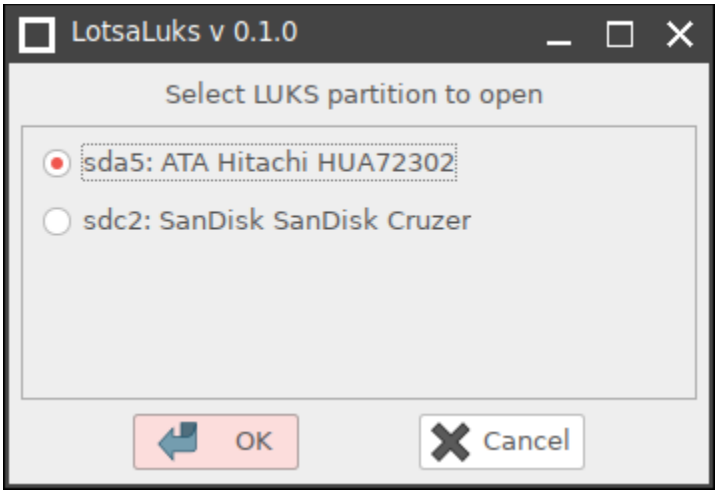
(From here on “LotsaLuks” will be referred to as “the app”.)

The app can create LUKS encrypted disks, encrypt individual disk partitions, and create encrypted filesystems in the form of files that can be mounted as loop devices. It can also quickly change the LUKS passwords of all your LUKS items, ”on the fly”. This means you can quickly and easily change the passwords on your LUKS savefiles while they are still in use.

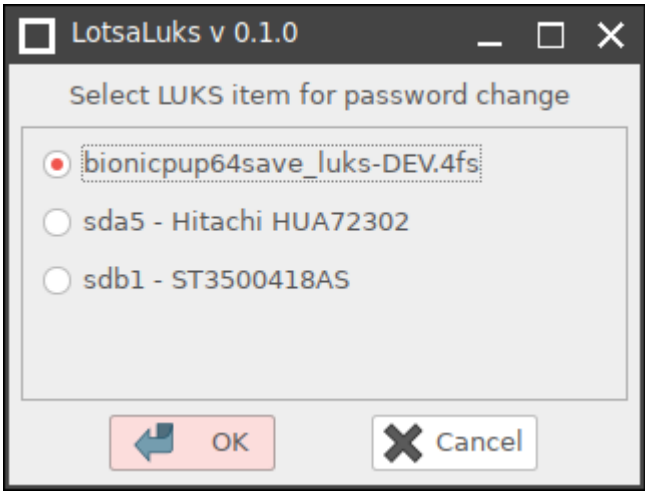


Encrypted items opened by the app are mounted under '/luksmnt’ by default. (You can, however, change that behavior by editing the "MountRoot” variable in the app’s script.)

Opened items are named either by their device name (sdc1, etc.), or the filename (without the extension) . If a filename contains spaces, the app replaces the spaces with underscores to create it's device name.



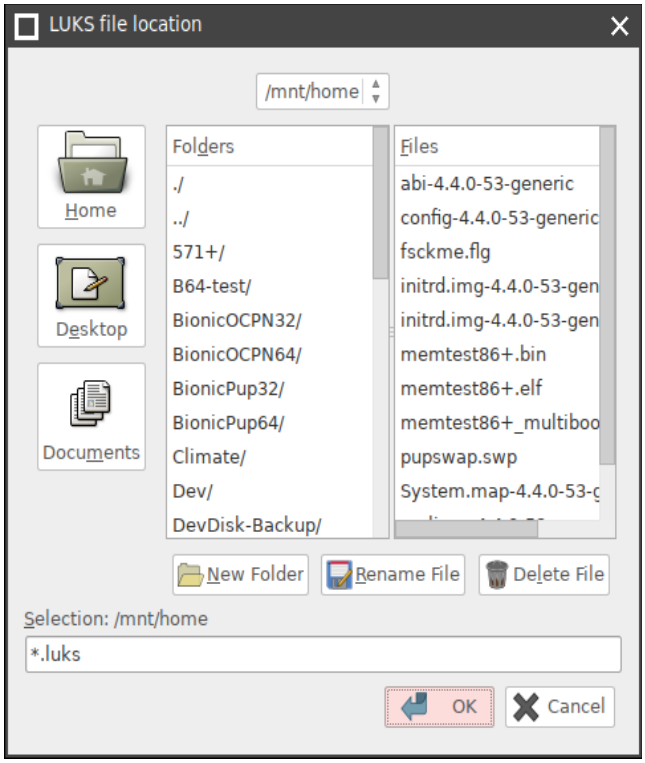
The app is homogeneous, meaning it only concerns itself with closing the items it opens, etc., except for changing passwords.



The app will change the password of *any* LUKS encrypted item, and it will do it on the fly.

The one exception to this is that you will want to open LUKS files *first*, before changing the password so that the app will be aware of their existence.

When you select the item to change, you will be prompted for the current password, then for the new password twice. It will change the password even if the item is mounted, and you will need the new password the next time you open the item.

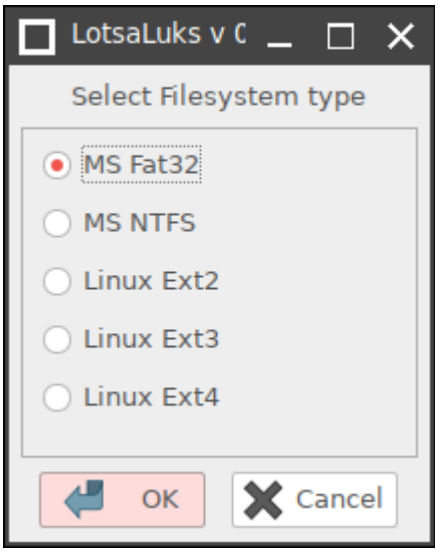


Creating/opening of LUKS files is performed through the same dialog. It defaults to '/mnt/home' because the app assumes you do **NOT** want to create the encrypted file inside Puppy's personal storage.

Pick a location and name. You will be prompted for the size in megabytes to make it.

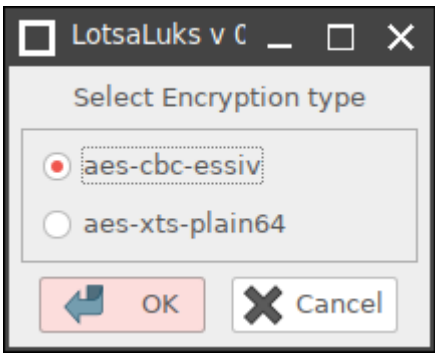
NOTE: A LUKS file can have any file name, but the app will "suggest" a ".luks" extension for clarity.

It is strongly suggested to keep LUKS encrypted files either in the same place as your '.sfs' files, or on separate disk media/partitions!



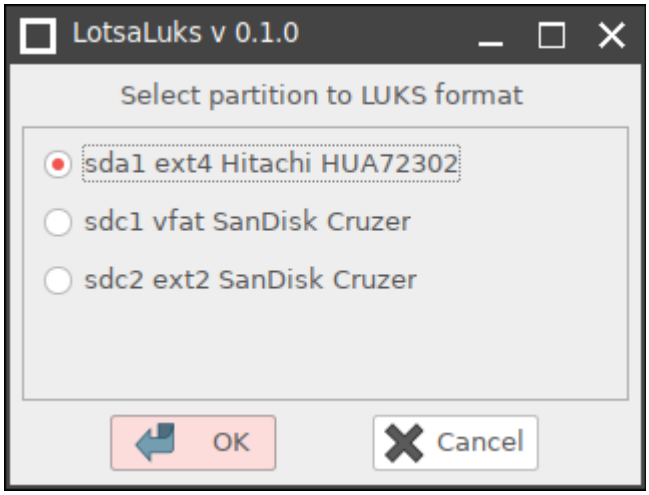
When creating a LUKS disk, partition, or file, you will be prompted to specify the filesystem type you want for the item you are creating.

As you can see, the options are fairly robust, and should meet the needs of most purposes.



After you make that selection, you will be prompted to select the encryption suite you require.

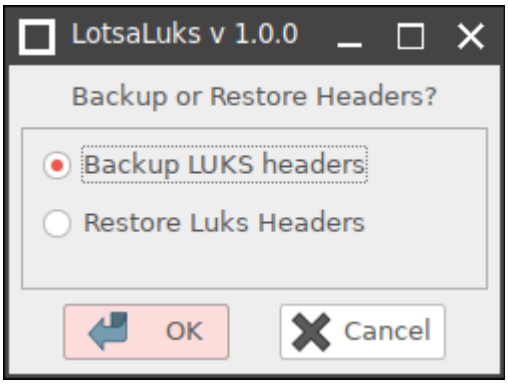
Keep in mind that if you have machines with older variants of Cryptsetup/LUKS (Precise 5.7.1 comes to mind), you will want to use the default (aes-cbc-essiv) to ensure they will be able to use that new item. If you don't have older OS's using LUKS, use the newer and stronger "plain64" suite.



When formatting either entire disks, or just a disk partition, the app will present you with a list of candidate targets that are not already LUKS devices.

If you want to reformat an existing LUKS disk or partition, use GParted to remove the LUKS partition first.

Depending on user consensus, this behavior can/may be changed.



And finally, the app can be used to backup and restore the LUKS Headers for your LUKS disks, partitions, and files, including your “pupsave_luks” files.

The backed-up header files are automatically saved into the “/luksmnt/.headerbackup” as a default that can be changed in the “HeaderPath="$MountRoot/.headerbackup"” variable in the LotsaLuks script.

The fact that the directory is hidden keeps it from being deleted by scripts (like “delete-stale-mounts”) that do mountpoint housekeeping.

Why is this important? Because the primary cause of data loss to LUKS volumes is due to some process, or user, accidentally damaging the LUKS headers that describe how to decrypt the volume. An excerpt from the cryptsetup man page:

“If the header of a LUKS volume gets damaged, all data is permanently lost unless you have a header-backup. If a key-slot is damaged, it can only be restored from a header-backup or if another active key-slot with known passphrase is undamaged. Damaging the LUKS header is something people manage to do with surprising frequency. This risk is the result of a trade-off between security and safety, as LUKS is designed for fast and secure wiping by just overwriting header and key-slot area.”

The header backups DO NOT contain the passphrases needed to open the volume, just the metadata needed to do so. Keep them somewhere safe.

The app makes a fairly rigorous effort to name the backups according to the device name/product name/filename of the volume . Feel free to rename these to whatever will better suit your needs, if necessary.