Backup and Restore Volume Header

5-6 minutes ⋮ %published-time%

If the header of a VeraCrypt volume is damaged, the volume is, in most cases, impossible to mount. Therefore, each volume created by VeraCrypt (except system partitions) contains an embedded backup header, located at the end of the volume. For extra safety, you can also create external volume header backup files. To do so, click *Select Device* or *Select File*, select the volume, select *Tools* -> *Backup Volume Header*, and then follow the instructions.

Note: For system encryption, there is no backup header at the end of the volume. For non-system volumes, a shrink operation is done first to ensure that all data are put at the beginning of the volume, leaving all free space at the end so that we have a place to put the backup header. For system partitions, we can't perform this needed shrink operation while Windows is running and so the backup header can't be created at the end of the partition. The alternative way in the case of system encryption is the use of the Rescue Disk.

Note: A backup header (embedded or external) is *not* a copy of the original volume header because it is encrypted with a different header key derived using a different salt (see the section *Header Key Derivation, Salt, and Iteration Count*). When the volume password and/or keyfiles are changed, or when the header is restored from the embedded (or an external) header backup, both the volume header and the backup header (embedded in the volume) are re-encrypted with header keys derived using newly generated salts (the salt for the volume header is different from the salt for the backup header). Each salt is generated by the VeraCrypt random number generator (see the section *Random Number Generator*).

Both types of header backups (embedded and external) can be used to repair a damaged volume header. To do so, click *Select Device* or *Select File*, select the volume, select *Tools* -> *Restore Volume Header*, and then follow the instructions.

WARNING: Restoring a volume header also restores the volume password and PIM that were valid when the backup was created. Moreover, if keyfile(s) are/is necessary to mount a volume when the backup is created, the same keyfile(s) will be necessary to mount the volume again after the volume header is restored. For more information, see the section *Encryption Scheme* in the chapter *Technical Details*.

After you create a volume header backup, you might need to create a new one only when you change the volume password and/or keyfiles, or when you change the PIM value. Otherwise, the volume header remains unmodified so the volume header backup remains up-to-date.

Note: Apart from salt (which is a sequence of random numbers), external header backup files do not contain any unencrypted information and they cannot be decrypted without knowing the correct password and/or supplying the correct keyfile(s). For more information, see the chapter *Technical Details*.

When you create an external header backup, both the standard volume header and the area where a hidden volume header can be stored is backed up, even if there is no hidden volume within the volume (to preserve plausible deniability of hidden volumes). If there is no hidden volume within the volume, the area reserved for the hidden volume header in the backup file will be filled with random data (to preserve plausible deniability).

When *restoring* a volume header, you need to choose the type of volume whose header you wish to restore (a standard or hidden volume). Only one volume header can be restored at a time. To restore both headers, you need to use the function twice (*Tools* -> *Restore Volume Header*). You will need to enter the correct password (and/or to supply the correct keyfiles) and the non-default PIM value, if applicable, that were valid when the volume header backup was created. The password (and/or keyfiles) and PIM will also automatically determine the type of the volume header to restore, i.e. standard or hidden (note that VeraCrypt determines the type through the process of trial and error).

Note: If the user fails to supply the correct password (and/or keyfiles) and/or the correct non-default PIM value twice in a row when trying to mount a volume, VeraCrypt will automatically try to mount the volume using the embedded backup header (in addition to trying to mount it using the primary header) each subsequent time that the user attempts to mount the volume (until he or she clicks *Cancel*). If VeraCrypt fails to decrypt the primary header but it successfully decrypts the embedded backup header at the same time, the volume is mounted and the user is warned that the volume header is damaged (and informed as to how to repair it).