

Setting Hardware Locks

Hardware locks serve as programmable blocking of reading and writing to selected memory area. The use of hardware locks is an efficient measure for protecting dongle contents.

Setting of hardware locks is done on the lower level. This guarantees the impossibility to break them using the common software means. The dongle will simply not respond to attempts to read/write into protected memory area.

Important information

In the recent models of Guardant dongles, you can gain access to protected items (special category of locked memory fields) using special Guardant API functions.

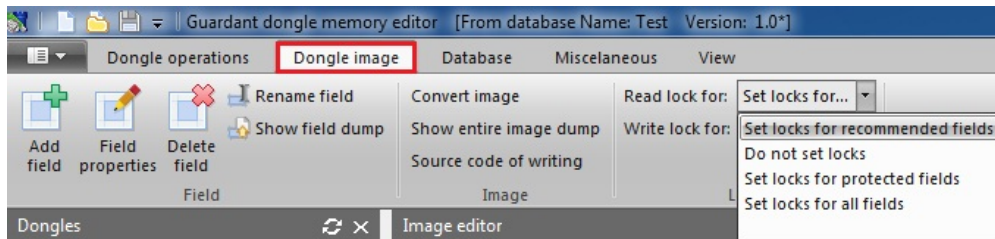
The locks can be set on a continuous freepurpose memory area starting with lower addresses (i.e. from address 14 UAM to the area of special operation fields).

GrdUtil.exe will automatically set read/write locks on the fields of the following types: hardware algorithms, protected memory items, the license table.

Important information

It is strongly recommended to lock for reading and writing the memory areas used by hardware algorithms, license tables and protected memory items!

In order to set hardware locks, execute command **Dongle | Set Read/Write locks** from the menu. The current hardware locks are shown in **Read/Write locks Setting** dialog box that will appear:



The numbers in the entry fields indicate the address of the last byte (in UAM mode) protected against writing and reading respectively.

In order to change the size of the locked memory area, edit the values in the required entry fields.

You can set locks selectively (against reading only, against writing only) as well as combine them (both against reading and writing).

Types and indications of hardware locks in Mask Editor:

Hardware lock	Description
r	Locks the entire field against reading
r-	Partially locks the field against reading
w	Locks the entire field against writing
w-	Partially locks the field against writing
rw	Locks the entire field against reading and writing
r-w-	Partially locks the entire field against reading and writing

According to Guardant dongles ideology, the setting of the new hardware locks leads to the dongle memory initialization, i.e. all user's data will be deleted from the memory.

Thus, after setting the new parameters of locks in Mask Editor and writing mask into the dongle, the dongle memory gets completely updated. The following sequence of Guardant API operations is performed in this case:

- Dongle memory gets purged (GrdInit operation)
- Information from the mask is written into dongle (GrdWrite operation)
- Hardware locks are set on the selected memory area (GrdProtect operation)