HDGUARD 9 reference manual

RDT Ramcke DatenTechnik GmbH

Publisher:

RDT Ramcke DatenTechnik GmbH

Bergstraße 23

23843 Neritz

Tel: +49 (0) 4531 880 440

Fax: +49 (0) 4531 880 444

Email: info@rdt.de

Web: www.rdt.de

RDT Ramcke DatenTechnik GmbH

HRB 1408, OD Lübeck

CEO Victor Baum

Table of Contents

Overview....3
HDGUARD....3
HDGUARD.master....3
HDGUARD....4
Remarks and installation....5
Preparation....5
System requirements....5
Installation....5
Installation via graphical user interface....5
Installation into a cloning master....6
Installation and setup of a multi-boot system....6
Test period, licensing and software activation....7
Guide for the graphical user interface....8
First start....8
Configuration....8
Automatic hard disk configuration....8
Hard disk....9
License & passwords....9
Visibility....10
Update periods....10
Exceptions....11
USB mass storage....11
Help & miscellaneous....11
Main Window....12
Automatic mode....12
Seminar mode....12
Deactivate....12
Apply Changes....13
Guide for command line interface....13
Example: ListPartitions....15
Configuration via Registry (Cloning)....16
HDGUARD.master connection....17

Overview

HDGUARD

HDGUARD protects your hard drives against permanent changes. After restarting the computer, the desired original state is automatically restored. Even if users make changes to files or delete them, this has no permanent effect. The high level of operating safety of the protected PCs relieves the responsible IT employees of some of their burden and provides an extremely long-term period of stability – even for public PCs!

The protective effect of HDGUARD is augmented by an effective USB protection, which restricts the use of USB drives. A number of useful options also ensure that the software can be easily integrated into existing IT concepts. This makes HDGUARD suitable for virtually any area of application.

HDGUARD.master

The HDGUARD.master module centralizes the control and monitoring of HDGUARD-protected computers in your network. You can selectively activate and deactivate individual computers or entire rooms. Automatically monitor the protection of your computers and display safety warnings if a computer is started up unprotected.

HDGUARD.master perfectly supplements all networks where HDGUARD-protected PCs are used.

> HDGUARD is a pure software solution. No hardware interventions into the protected systems are required. So you do not need any PC cards or dongles. HDGUARD fits in perfectly in new or existing systems.

HDGUARD

HDGUARD protects your hard drives against permanent changes. After restarting the computer, the desired original state is automatically restored. Even if users make changes to files or delete them, they will not effect the system permanently. The high level of operating safety of the protected PCs relieves the responsible IT employees of some of their burden and provides an extremely long-term period of stability – even for public PCs!

This high level of operating safety is achieved by the fact that HDGUARD redirects all changes in the Windows partition (and in any other desired partitions) to the HDGUARD area. While the operating system is running, all functions can be used without restrictions, and the user does not detect any difference between this and a traditional unprotected PC. As soon as the PC is restarted, HDGUARD discards all changes. This requires only a fraction of a second, no matter how extensive the changes were.

The protective effect of HDGUARD is augmented by an effective USB protection, which restricts the use of USB drives. A number of useful options also ensure that the software can be easily integrated into existing IT concepts. This makes HDGUARD suitable for virtually any area of application.

Beyond the classic protection features a few of helpful and didactic features have been added to the HDGUARD product family. So to get the most out of your IT equipment, see the chapters titled t*eacher console* and *configuratio*n.

Remarks and installation

Preparation

System requirements

Usual 32- or 64-Bit PC with at least 2 GB RAM and 50 GB hard drive or SSD.

Operating system: Microsoft Windows XP SP3, Microsoft Windows XP x64 SP2, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8 or Microsoft Windows 8.1 plus the according Server variants.

Hard disk setup: MBR- or GPT with primary and secondary partitions.

Volume formatting: FAT32[1], NTFS

Free space: At least 4 GB free coherent space on *C:*, recommended at least 20 GB free coherent space on *C:*.

RAID-systems or similar partition accumulations like *dynamic volumes* are not supported.

Installations into virtual machines are not supported!

HDGUARD protects the data on the hard drive basically per partition. This means, that all changes to Registry entries and to files on system volume *C:* are always being restored at each reboot. HDGUARD provides some helping functions for some scenarios for which these limitations are being eased. Therefore an additional partition on your system hard disk is necessary. This partition can be subsequently created by Windows Disk Management[2]. You can find more information on this in chapter *exceptions*.

Installation

First, make backup copies of all important data. Faulty operation, incorrect installation or an unscheduled interruption of the installation or configuration could result in damage to or loss of data. RDT Ramcke DatenTechnik GmbH and its partners are not responsible for any loss of data or the consequences thereof.

Installation via graphical user interface

Save all open documents and close all running applications before proceeding.

Execute on a 32-Bit Windows installation *HDGUARD 9.x.x.x - 32Bit.msi* and on a 64-Bit Windows installation *HDGUARD 9.x.x.x - 64Bit.msi* . You can download the actual setup files at *www.hdguard.com* . Once HDGUARD has been installed completely, you will see a message box asking for a reboot. This reboot is required, in order to start up HDGUARD.

1 Due to systemic limitations it is advised, not to use FAT32.
2 Beginning with Microsoft Windows Vista

Installation into a cloning master

Set up the operating system and install all your desired applications.

Execute on a 32-Bit Windows installation *HDGUARD 9.x.x.x – 32Bit.msi* and on a 64-Bit Windows installation *HDGUARD 9.x.x.x – 64Bit.msi*. You can download the actual setup files at *www.hdguard.com* .

Configure HDGUARD by using the HDGUARD user interface. You must not configure any hard drive partitions. After the clone process an automatic hard drive configuration will be performed. Setting up the passwords and the software activation must be done after cloning. This can be done automatically, please read section “Configuration via Registry”.

Now create the image for cloning.

HDGUARD **must not** be cloned with configured hard disk partitions!

For configuration afterwards you can additionally use the command line application *HDGcmd.exe* or the module HDGUARD.master.

Installation and setup of a multi-boot system

HDGUARD supports multi-boot systems with the Windows boot manager.

In order to set up such a system, use the following guide:

First insert the setup DVD of the highest to be installed Windows version and start its setup. In the partitioning screen click on *Drive Options (advanced)* and delete all partitions on your boot hard drive. Click on *new* and type in the size for the system partition *C:* for this Windows Version. Then create partitions for every other to be installed Windows version and additionally a partition for unprotected data.

When you have finished partitioning, do not click on *Next*. Instead remove the setup DVD or CD and insert the setup DVD or CD of the oldest Windows version, you want to integrate into the multi-boot system. Then reset the system. Install all Windows versions beginning from the oldest towards the newest Windows version into the designated partitions. Linux-Systems can be integrated as well. These installations must write their boot code into the start sector of their boot partition and have to be registered into the Windows boot manager. (You can find guides for that in the internet.)

This procedure ensures, that the actual Windows boot manager is used and that you neither have to repair existing systems nor external tools need to be used. After all Windows systems have been installed and configured, install on each Windows system HDGUARD. Then configure HDGUARD on one Windows system. Please note that every partition, that contains a Windows installation, has to be set to mode *to protect*. Eventually existing (hidden) start partitions have to be configured as “read only”.

This HDGUARD configuration applies to all Windows installations on the multi-boot system. So you have to do it only once for the whole system. Software activation (see next chapter) applies to all installations, too.

After you have completed your HDGUARD configuration, execute HDGUARD on all Windows installations beginning on the oldest Windows version and click on *Activate* and *Automatic* or *Seminar mode*. Choose *No* when you are asked for protection in a multi-boot system. When you have reached your newest Windows version, choose *Yes*.

This ensures, that all Windows installations are prepared for the HDGUARD protection.

Test period, licensing and software activation

After the installation of HDGUARD you have 30 days left to test the software without a serial number. Within this time period you can use all functions except the change of the visibility and password protection.

If you type in a valid serial number, you will get the full functionality until 60 days after installation.

Unlimited functionality is provided after you have done an online registration of every HDGUARD installation at RDT (software activation). Therefore a data packet containing HDGUARD serial number and identification of the hardware will be sent to a server of RDT. This server generates an answer, which activates unlimited functionality of your HDGUARD installation. This answer does not only contain the information of the activation, but also might provide updated licensing information.

This exchange of data can be done, when your PC has a direct (or proxy-) internet connection. Both the HDGUARD graphical user interface and the `HDGcmd.exe` command line tool can perform this task. If you do not have an internet connection, both applications can generate a request file. This file will be accepted on the internet site `https://activation.xmood.de/HDGUARD` . This site will generate a computer specific answer file, which will be accepted by both mentioned applications.

Unlike the software activation process of Microsoft Windows or Microsoft Office, RDTs software activation can be performed unlimited times on the same PC without “consuming” further client license counts. Even a re-installation of HDGUARD with repeated software activation on the same PC does not “consume” any further license count, if the hardware does not change.

Because the software activation updates the license information, a time limited testing license can be renewed for instance, so it can be used for some extra months or it can be changed into a commercial license without changing the serial number.

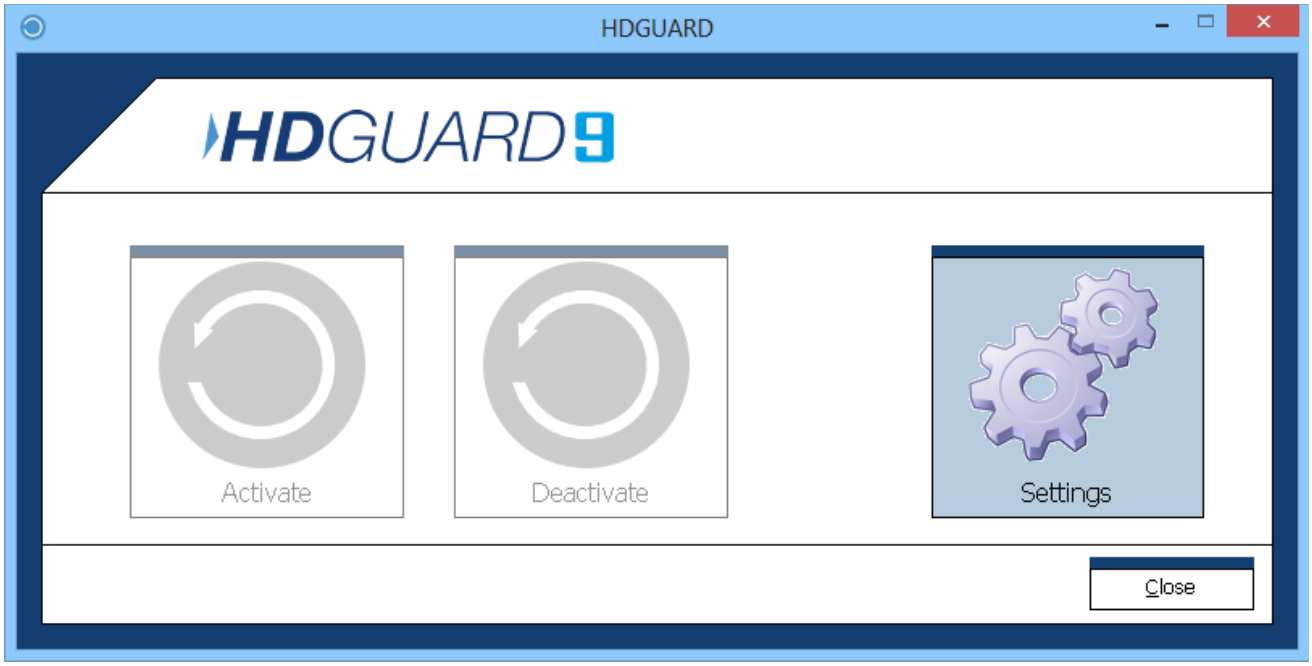
You need one HDGUARD license per computer. The same applies to multi-boot systems.

Guide for the graphical user interface

Once installation has been completed you find HDGUARD on the desktop, in 'Start Menu' and in its program folder.

First start

Double-click the HDGUARD symbol in order to open the central user interface. You will see the main window with its deactivated control buttons.



Press *Settings* in order to open the configuration window.

Configuration

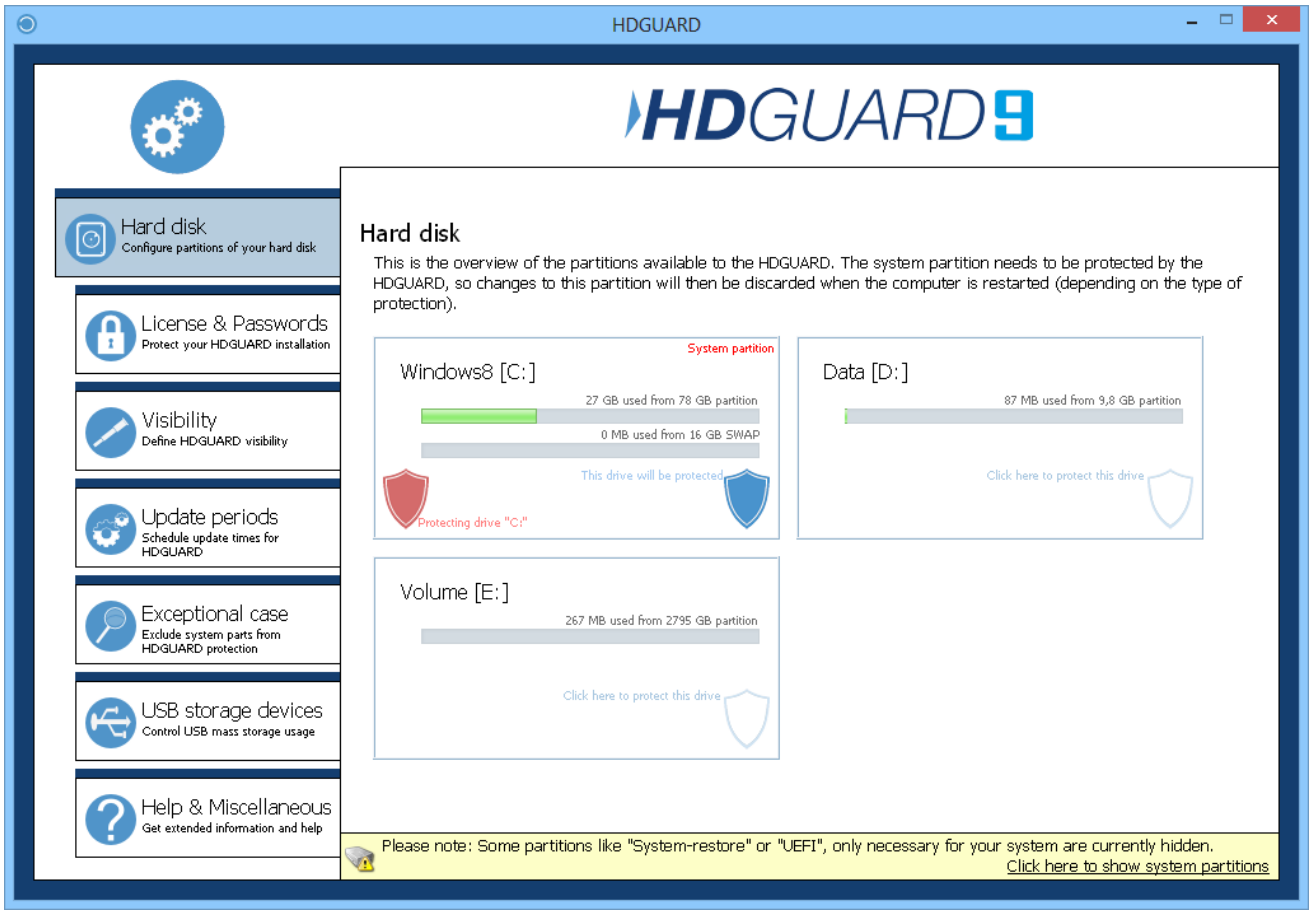
The configuration screen contains everything you need for customizing HDGUARD to suit your needs. In most cases, you will only need the configuration screen once before activating HDGUARD. Thereafter, changes to the configuration will only need to be made in rare instances.

Automatic hard disk configuration

When you start HDGUARD application on a PC without configured HDGUARD protection, an automatic configuration will be made. This will set the protection mode of eventually existing starting- and boot-partitions to *Read only* and creates a SWAP-file for the protection of Volume *C:*.

Hard disk

This is where you define which partitions are supposed to be protected and where the corresponding HDGUARD SWAP-files will be located.



If you want to enable HDGUARD protection for volume `D:`, just click into the field representing volume `D:`. You will be asked for the protection mode, which can be *"to protect"*, "*read only"* or *"no access"*.

Choosing *"to protect"*, a protection configuration window opens and you can adjust all available related options. These options contain:

- Where the SWAP-file is located? It must be placed on the same hard disk.
- How much space should be allocated for the SWAP-file on the designated partition? File system has to provide a continuous area for the SWAP-file.
- How many RAM should be reserved in order to speed up the beginning of the SWAP area? Available only for system partitions.

License & passwords

Here you can type in your serial number and initiate or repeat the software activation process. If the local PC cannot establish a connection to the RDT activation server, you can save the request into a file, you can send to RDT by e-mail.

In the second tab (which can be accessed by clicking *Next* or *Back*) you can set the HDGUARD password.

> Make sure that you do not forget your HDGUARD password. There are no master passwords or possibilities for password restoration!

In the third tab you can set the password for resetting the seminar mode. Without this password every user can reset the seminar mode.

In the fourth tab you can define USB storage devices. If one of these devices is plugged in, HDGUARDs password protection will temporarily be overridden[3].

Visibility

Links in the start menu and on the desktop plus the appearance of the system tray icon can be adjusted here.

Update periods

Within these periods the PC starts without HDGUARD protection but with restrictive log-on policy. Log-on to the PC is not allowed, except it is the account which is defined in the fourth tab. You can also do unattended Windows updates and start executable files. For these executables and for the automatic log-on with locked screen you can provide log-on credentials in the fourth tab.

In the first three tabs you can adjust starting time, duration, log-on options and further actions of the three independent update periods.

If the installation of Windows updates exceeds the duration of the actual update period, the period will be automatically extended.

> Some Windows updates need a restart of the machine. HDGUARDs service initiates a reboot after such updates have been installed. If you are logged on as a permitted user within such an update period, this reboot will terminate your session without request!

HDGUARD automatically recognizes time changes caused by Windows' daylight saving time configuration. The first start after a time change leads to a special update period, that ends after approx. two minutes. No one can log-on within this update period. After an automatic restart HDGUARD protection is reactivated.

3 Password changes and learning further Service Keys are prohibited.

Exceptions

HDGUARD inherently protects your hard drive per partition. So basically you cannot make exceptions for files or folders from the HDGUARD protection within a protected partition. The same applies to keys and values in Registry, which is stored in multiple files on system partition *C:*.

HDGUARD implements two techniques that allow limited exceptions for folders and Registry keys. Therefore you need an additional NTFS formatted partition, that is not protected by HDGUARD.

Exceptions for folders are set up as (NTFS-) junctions by HDGUARD configuration. The folder obviously lies on the protected partition, the NTFS file system though reroutes access to a hidden folder on the unprotected partition.

Exceptions for Registry Keys are realized as periodical backups of the specified Registry keys which are saved into files on the unprotected partition. These backups are restored at late boot time. So you cannot make an “exception” for keys that are relevant for your systems boot process. You cannot set up exceptions for keys that are not loaded at late boot time like keys of the hive of the current user HKCU.

USB mass storage

HDGUARD contains a special handling for USB devices of the class USB mass storage. These devices can be write protected or access protected. Additionally HDGUARD can eject those devices directly after they are plugged in.

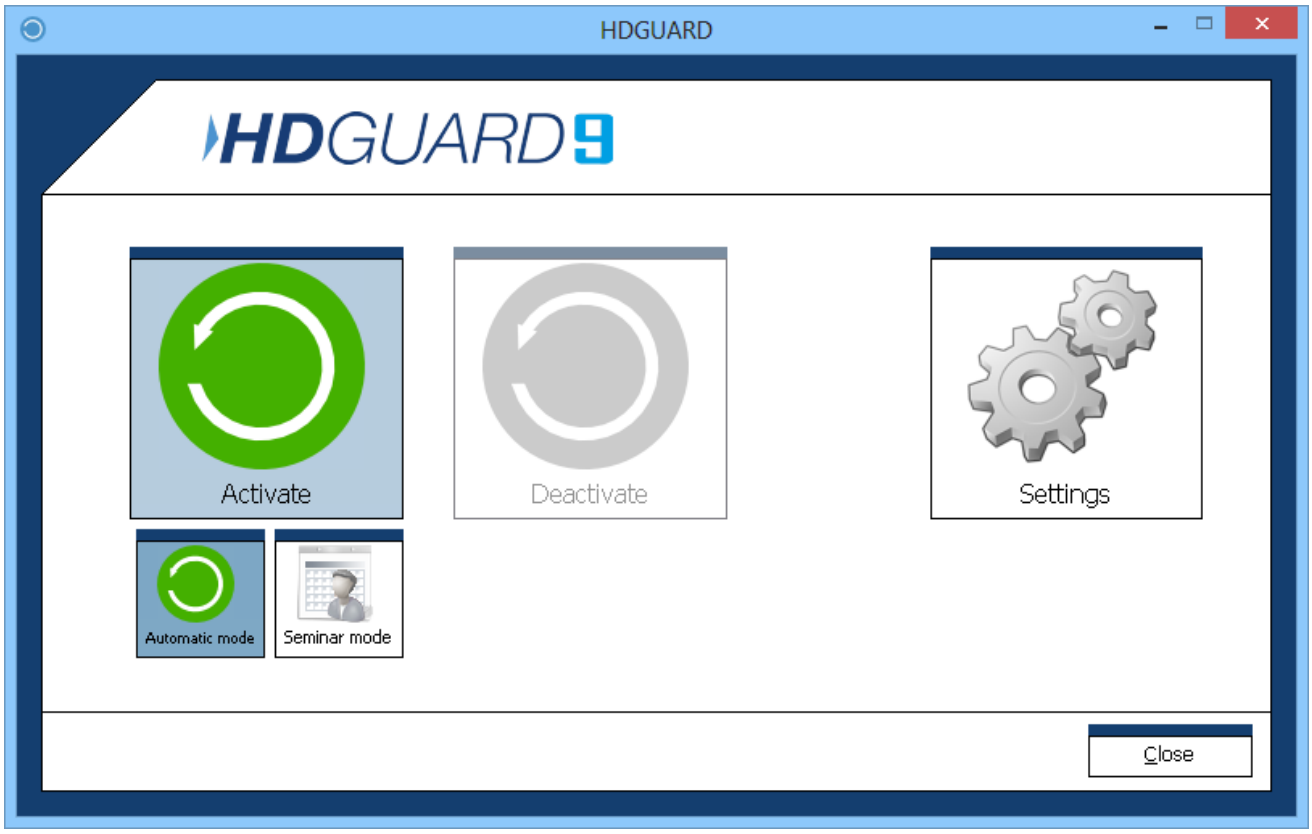
Not all devices with file and folder access belong to the class USB mass storage. Therefore HDGUARDs configuration contains an option for including USB devices of type “unknown” into the eject function. But this option may cause that other USB devices are being ejected, which have no storage functionality.

Help & miscellaneous

This configuration tab does not only show version and licensing information, but provides also the possibility to go to the product web site or send feedback to the developers.

Main Window

If you leave the configuration menu, you see the main window again. After you have completed the hard disk configuration, protection can be activated.



Automatic mode

If you choose *Activate – Automatic mode*, the system will first be prepared for the HDGUARD protection. Then the system reboots and the protection is activated. Every reboot of your PC resets its state to this initial state that you have defined by clicking “Activate”.

Seminar mode

If you choose *Activate – seminar mode*, functionality differs from the previous one in that a reboot normally does not restore the state of the system. The actual state is preserved as long as either

- free space of one HDGUARD SWAP-file exceeds or
- a user clicks *reset seminar mode* in the context menu of the HDGUARD system tray icon or
- an update period begins, which priority is higher than the seminar mode.

Deactivate

If you choose *Deactivate – Deactivate*, HDGUARDs protection ends by rebooting the system. This restores the original state of the PC.

Apply Changes

If you choose *Dectivate – Apply changes*, protection will be disabled on the fly making the actual state of the specified partitions permanent at runtime. This may take a while, because data from the SWAP-files is copied into the protected partitions.

Guide for command line interface

You can control HDGUARD via command line, too. Therefore run the executable file HDGcmd.exe in the program folder with the desired command line option. Running it without or wrong options, it shows the command line help:

```
HDGUARD command line tool

HDGCMD [command [PWD] [option1 [option2 ...]]]]

Numeric values are returned by ERRORLEVEL environment variable!
Negative return values indicate an error.
Return value 0 usually indicates success.

PWD and its variations are placeholders for encrypted passwords!
Note: The (initial) empty password "" must be encrypted aswell.

Example 1:
> HDGcmd /EncryptPWD ""
ndwevu7Msgu4/IZgOrznSOETN7vh9iRU8djZ+oQjs/shMH/M4+gkN4jCJ+R6VasS

Example 2:
> HDGcmd /EncryptPWD "MyS3cr3tPassw0rd"
hEb8CLS8S4saLdJgzt3QCC51sRja+DTpd4mwxqb/PBfQdWDGdcAH4Qe8+PKdcd7+

The following commands are allowed:
/EncryptPWD "password"      :Encrypts the given password.
                             Use the output for PWD placeholders.
/DecryptPWD PWD             :Decrypts password PWD.
/SetUserPassword PWD UPWD   :Sets the user password.
/SetPassword PWD newPWD     :Sets the normal password.
/SetMasterPassword MPWD newMPWD
                            :Sets the master password.
/GetMode                    :Returns the actual protection mode:
                             0 -> Protection disabled
                             1 -> Protection enabled
                             2 -> Seminar mode enabled
                             4 -> Automatic update period
                             5 -> Update period 1
                             6 -> Update period 2
                             7 -> Update period 3
/GetModeInConfig            :Returns the planned protection mode after reboot.
                             For return values see /GetMode
/ActivateProtection PWD     :Reboots the system and
                             activates normal HDGUARD protection.
/ActivateSeminarMode PWD    :Reboots the system and
                             activates the seminar mode.
/DeactivateProtection PWD   :Reboots the system and
                             deactivates HDGUARD protection.
/PrepareForProtection PWD   :Prepares the system for HDGUARD protection and
                             reboots. Only for secondary Windows installations
                             on multi boot systems!
```

```
/ApplyChanges PWD i          :Applies changes to the specified volume and
                              deactivates its protection temporarily.
                              Note: Global protection mode is not changed!
/SetSeminarReset PWD 0       :Reboot will not reset session
                              information of the seminar mode.
/SetSeminarReset PWD 1       :Reboot will reset session information
                              of the seminar mode.
/GetSeminarReset             :Returnes reset session value of the
                              seminar mode. (see /SetSeminarReset)
/ListPartitions              :Shows information about hard drive partitions.
                              Use this command to retrieve the reference index i
                              for each partition
/AutoConfig PWD              :Tries to do an automatic volume configuration.
/ResetVolume PWD i           :Resets the HDGUARD protection mode of the volume
                              referenced by index i.
/SetVolumeProtected PWD i t s r
                             :Sets the HDGUARD protection mode of the volume
                              referenced by index i to PROTECTED.
                              t: Index of the volume to hold the swap file.
                              t usually equals i.
                              s: Size of the SWAP-File in MB.
                              s is usually set to 16384.
                              r: Size of the SWAP-Ram in MB.
                              r is usually set to 32 for C: and to 0 otherwise.
/SetVolumeReadOnly PWD i     :Sets the HDGUARD protection mode of the volume
                              referenced by index i to READ_ONLY.
/SetVolumeNoAccess PWD i     :Sets the HDGUARD protection mode of the volume
                              referenced by index i to NO_ACCESS.
/GetUsage i                  :Returnes the usage of the SWAP-File protecting
                              the volume referenced by index i in percent.
/SetLicense PWD XXXXXXXXXXXXXXXXXXXX
                             :Sets the license number for this installation.
                              Do not type in spaces or dashes!
/RequestFileActivation "FULL_PATH_TO_FOLDER"
                             :Saves an activation request file into the specified
                              folder. Use it for manual software activation.
/SetActivationAnswer "FULL_PATH_TO_FILE"
                             :Imports an activation answer file. Use it for
                              manual software activation.
/DoOnlineActivation          :Tries to do software activation via internet.
                              Use /SetWebProxy for proxy settings.
/SetVisibility PWD b b b b   :Four boolean (0 or 1) values, that enable
                              splash screen, system tray icon, mouse hover
                              window of the system tray icon and
                              context menu of the system tray icon.
/SetStartmenuLink b          :Boolean (0 or 1) value b, that enables HDGUARD
                              start menu entries.
/SetDesktopLink b            :Boolean (0 or 1) value b, that enables HDGUARDs
                              desktop link.
/SetWebProxy PWD [ProxyNameOrIP Port ["ProxyLoginName" "ProxyPassword"]]
                             :Sets the proxy values for internet connections.
```

Example: ListPartitions

```
C:\Program Files\RDT Global\HDGUARD>HDGcmd.exe /ListPartitions
--------------------------------------------------------------------------------
HDGUARD index 2
Hard drive 0, partition 1: \\?\Volume{d371bdbf-7c4c-45e6-a9d3-6e1590ae93ee}\
Size: 300 MB, free space: 78 MB
HDGUARD mode: 1 (READ_ONLY)
--------------------------------------------------------------------------------
HDGUARD index 3
Hard drive 0, partition 2:
Size: 100 MB
HDGUARD mode: 1 (READ_ONLY)
--------------------------------------------------------------------------------
HDGUARD index 4
Hard drive 0, partition 3:
Size: 128 MB
HDGUARD mode: 1 (READ_ONLY)
--------------------------------------------------------------------------------
HDGUARD index 5
Hard drive 0, partition 4: C:\
Size: 79472 MB, free space: 52951 MB
HDGUARD mode: 2 (REDIRECTED),
SWAP-File size: 16384 MB on index 5, SWAP-Ram size: 32 MB
--------------------------------------------------------------------------------
HDGUARD index 6
Hard drive 0, partition 5: D:\
Size: 10000 MB, free space: 9912 MB
This volume is marked as target for folder exceptions and registry exceptions
--------------------------------------------------------------------------------
HDGUARD index 7
Hard drive 1, partition 1: E:\
Size: 2861587 MB, free space: 2861319 MB
```

Configuration via Registry (Cloning)

This section deals with the configuration help for cloned HDGUARD installations.

When you clone a HDGUARD installation the entire hard disk configuration will be lost. It is therefore recommended to clone before you configure your hard disks. Normally the first start after the cloning process will be detected and an automatic hard disk configuration be performed. This can be parametrized by registry settings.

Create the following Registry key, if it does not already exist:

`HKLM\SOFTWARE\RDT Global\HDGUARD\AutoReConfig\RedirVolumes`

Then add a DWORD or a QWORD value for each partition that is supposed to get the HDGUARD protection. Name the value with the appropriate path (e.g. `D:`) The value itself should be the size of the SWAP file in MB.

In any case there will be an automatic configuration performed for the Windows volume `C:` . In case you need a size of the SWAP file, that differs from the automatic predefinition, you should set the value for `C:` explicitly.

The hidden system partitions which are created automatically by the newer Windows versions will be automatically configured as “read only”.

If the HDGUARD password is set, it must be deposited in following key:

`HKLM\SOFTWARE\RDT Global\HDGUARD\AutoReConfig\EncPasswords`

The password is stored as `REG_SZ` values with the name `PWD` with the encryption of HDGcmd.exe (see previous section).

If a license key has been entered before cloning, the HDGUARD service is finally trying to connect via the internet with the software activation server of RDT in order to perform the software activation. If there is no direct internet connection you can provide the configuration for your proxy server with the key:

`HKLM\SOFTWARE\RDT Global\HDGUARD\AutoReConfig\InternetProxy`

The values are defined as the following:

- `REG_SZ` value named `ProxyNameOrIP` for the address or the name of the server
- `REG_DWORD` value named `Port` for the port of the connection
- If necessary `REG_SZ` value named `LoginName` for the login name of the connection
- If necessary `REG_SZ` value named `Password` for the associated password

The key

`HKLM\SOFTWARE\RDT Global\HDGUARD\AutoReConfig`

will be automatically deleted after the automatic configuration.

HDGUARD.master connection

In order to administer each HDGUARD client PC with the module HDGUARD.master a TCP/IP connection to the respective PC or server with installed HDGUARD.master central service has to be established. On the HDGUARD client PC this connection is an outbound connection.

The HDGUARD set-up therefore retrieves the appropriate name, IP or divergent connection port if necessary and stores them in the registry. Without explicit configuration following settings will be used:

- Name: `HDGUARDmaster`
- Port: `52234`

In larger networks it is recommended to use an alias name (CNAME) in the DNS server for the HDGUARD.master service PC.

If this is not possible or you do have to take a different port using the HDGUARD.master service, you can provide the configuration per command line to the HDGUARD set-up.

During an unattended installation the command line would look like this:

```
msiexec /i “HDGUARD 9.x.x.x – 64Bit.msi“ /q HDMADDRESS=MyHDGUARDmasterPC HDMPORT=50000
```

Subsequent changes of the configuration can only be done via the registry. Die `REG_SZ` values `SERVER` and `SERVERPORT` can be found in the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\RDT Global\HDGUARD`

The new settings will be read with the next reboot. Don’t forget to deactivate the HDGUARD temporarily before the restart!