HDGUARD 11 User Manual

HDGUARD 11 User Manual

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Publisher:

IST Deutschland GmbH
Bergstraße 23
D-23843 Neritz
Germany

Tel: +49 4531 8804-40
Fax: +49 4531 8804-44
Email: info.de@ist.com
Web: www.ist.com

IST Deutschland GmbH
HRB 1408, OD Lübeck
CEO: David Baunsgaard
© 2023 IST Deutschland GmbH

1 Introduction

1.1 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 teacher console and configuration.

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.

1.2 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.

2 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. IST Deutschland GmbH and its partners are not responsible for any loss of data or the consequences thereof.

If you want to install HDGUARD and (parts of) HDGUARD.master on the same system, you must install HDGUARD.master first.

2.1 Type of HDGUARD protection and imits

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. It is recommended to use update periods 18, in order to update or install software while HDGUARD protection is deactivated. In some cases you can use exceptions 22. Therefore an additional partition on your system hard disk is necessary. This partition can be subsequently created by Windows Disk Management.

Windows Update service is deactivated while HDGUARD protection is active. Operating system updates and Windows Defender updates can be installed only when HDGUARD protection is deactivated. Additionally Microsoft App-Store functionality is affected, if HDGUARD protection is active.

2.2 System requirements

2.2.1 Hardware

Standard PC with Intel x64 or AMD64 processor architecture and 4 GB RAM (recommended 8GB or more) and 128 GB hard disk, SSHD or SSD (recommended 180 GB or more).

Support for ARM64 processor architecture on Windows 11 systems.

RAID-systems and installations into virtual machines are not supported.

2.2.2 Operating systems

Microsoft Windows 10, version 2004 or newer
Microsoft Windows 11
Windows Server 2022

Each with architecture X86 and AMD64(x64)

Windows 11
For devices with ARM64 processor architecture

2.2.3 Hard disk setup

MBR or GPT with primary and secondary partitions.
HDGUARD can only include volumes with NTFS or FAT32 file system.

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

2.2.4 Free space

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

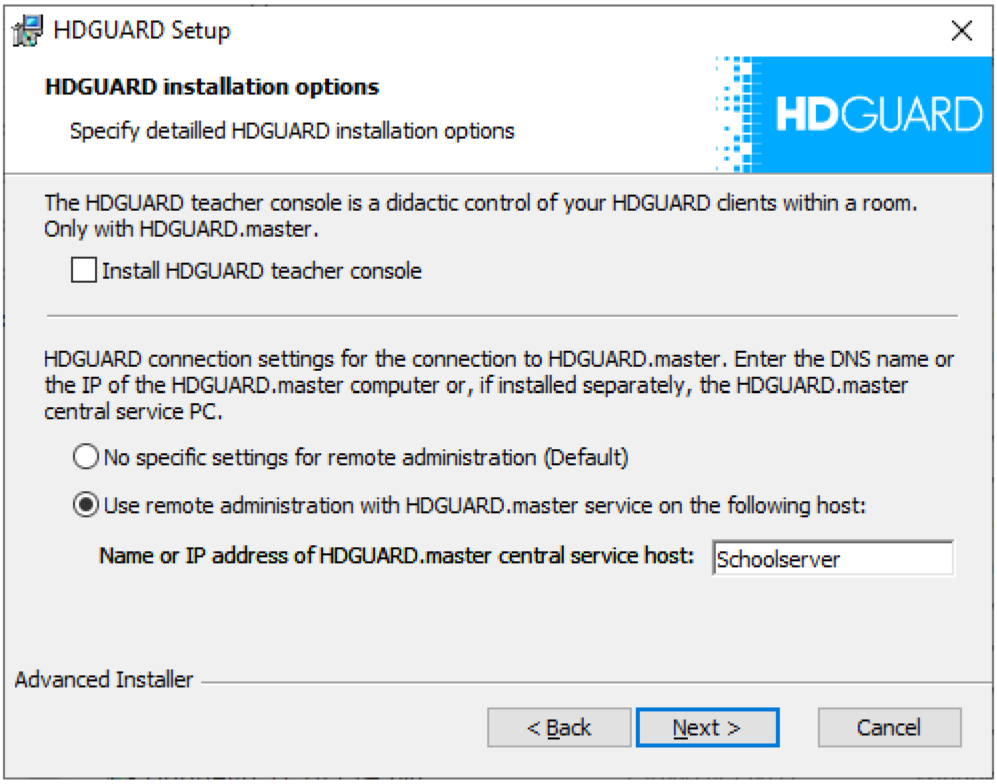
2.3 Installation with user interface

Save all open documents and close all running applications before proceeding..
Execute on a 32-Bit Windows installation HDGUARD11_32.msi and on a 64-Bit Windows installation HDGUARD11_64.msi. You can download current setup files at www.ist.com. Installer option teacher console 32 requires HDGUARD.master. Once HDGUARD has been installed completely, you will see a message box asking for a reboot.

This reboot is required before any further actions can be made.

If HDGUARD.master is used to manage the clients, the connection properties between the client and the central master service must be specified in the client setup. If no special settings are entered, the name HDGUARDmaster is used as the default. This is reasonable if the name of the PC on where the central service of the master is set up is HDGUARDMASTER, or a corresponding alias is entered in the DNS. This is also the appropriate setting for environments without the HDGUARD.master.

In all other cases, the second option must be selected and the name or IP of the PC on which the central service has been set up must be entered.


HDGUARD Setup

HDGUARD installation options

Specify detailled HDGUARD installation options

The HDGUARD teacher console is a didactic control of your HDGUARD clients within a room. Only with HDGUARD.master.

□ Install HDGUARD teacher console

HDGUARD connection settings for the connection to HDGUARD.master. Enter the DNS name or the IP of the HDGUARD.master computer or, if installed separately, the HDGUARD.master central service PC.

○ No specific settings for remote administration (Default)

● Use remote administration with HDGUARD.master service on the following host:

Name or IP address of HDGUARD.master central service host: Schoolserver

The teacher console 32 will only work in combination with the HDGUARD.master. It should be installed only on those workstations where teachers are working. As soon as HDGUARD is completely installed, a dialogue for restarting the computer appears.

Restarting the computer after installation is mandatory before further actions are carried out.

2.4 Installation into a cloning master

Set up the operating system and install all your desired applications.
Execute on a 32-Bit Windows installation `HDGUARD11_32.msi` and on a 64-Bit Windows installation `HDGUARD11_64.msi` . You can download current setup files at www.ist.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. Software activation must be done after cloning. This can be done automatically, please read section Helper functions for cloning 30.

HDGUARD must not be cloned with configured hard disk partitions!

Now create the image for cloning.
For configuration afterwards you can use command line application[27] HDGcmd.exe or HDGUARD.master additionally.

2.5 Installation and setup of a multi-boot system

HDGUARD supports multi-boot systems with 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 latest 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.

3 Licensing and test period

3.1 Test period

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 visibility[13] and password protection[12].

3.2 Licensing

If you type in a valid serial number[12], you will get the full functionality until 60 days after installation.

3.3 Software activation

Unlimited functionality is provided after you have done an online registration of every HDGUARD installation at IST Deutschland GmbH (software activation). Therefore a data packet containing

HDGUARD serial number and identification of the hardware will be sent to a server of IST Deutschland GmbH. This server generates an answer, which activates unlimited functionality of your HDGUARD installation. The 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://license-de.ist.com . This site will generate a computer specific answer file, which will be accepted by both mentioned applications. The connection in the automatic and manual activation of HDGUARD is encrypted according to the current state of the art.

Unlike the software activation process of Microsoft Windows or Microsoft Office, ISTs 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.

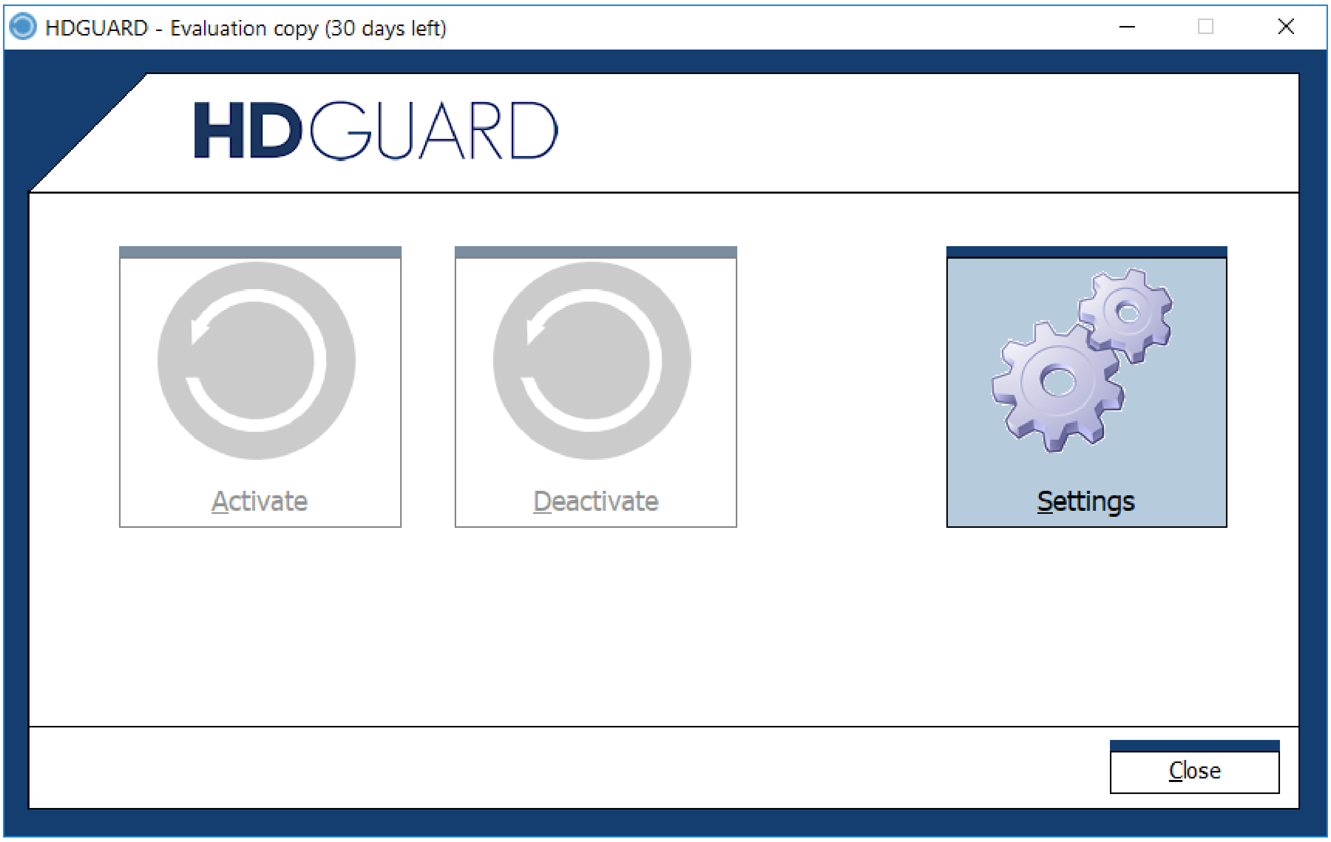
Because the software activation updates the license information, a time limited testing license can be renewed for instance, so it can be used for some extra months or it can be changed into a commercial license without changing the serial number.
You need one HDGUARD license per computer. The same applies to multi-boot systems.

4 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.

4.1 First start

Double-click the HDGUARD symbol in order to open the central user interface.
When you start HDGUARD application on a PC without configured HDGUARD protection, you will be asked, if an automatic configuration should be done. 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:.



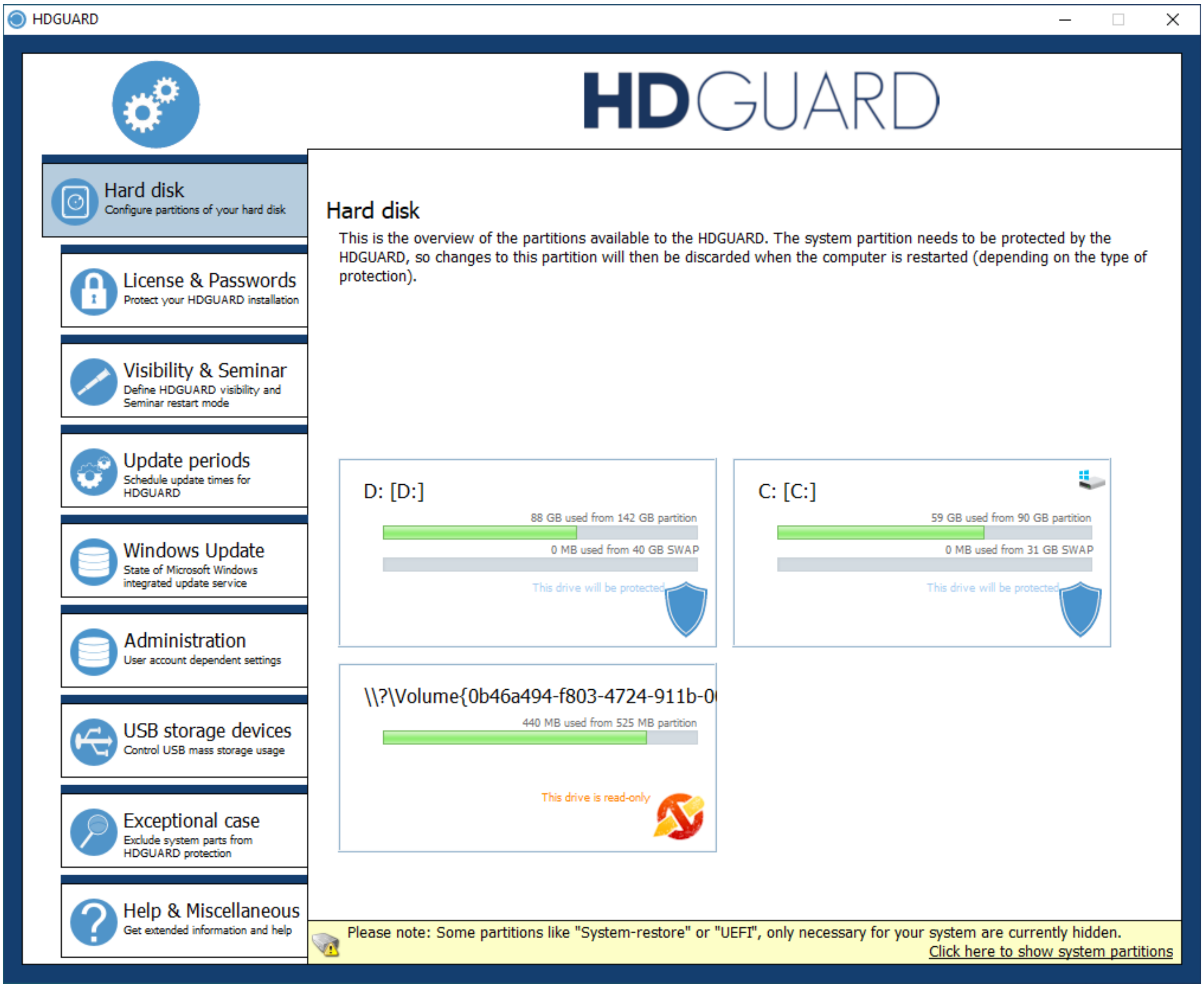
Main window with its deactivated control buttons.

4.2 Configuration

Press Settings in order to open the configuration window.
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.

4.2.1 Hard disk

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


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help

Hard disk

This is the overview of the partitions available to the HDGUARD. The system partition needs to be protected by the HDGUARD, so changes to this partition will then be discarded when the computer is restarted (depending on the type of protection).

D: [D:]
88 GB used from 142 GB partition
0 MB used from 40 GB SWAP
This drive will be protected

C: [C:]
59 GB used from 90 GB partition
0 MB used from 31 GB SWAP
This drive will be protected

\\?\Volume{0b46a494-f803-4724-911b-0
440 MB used from 525 MB partition
This drive is read-only

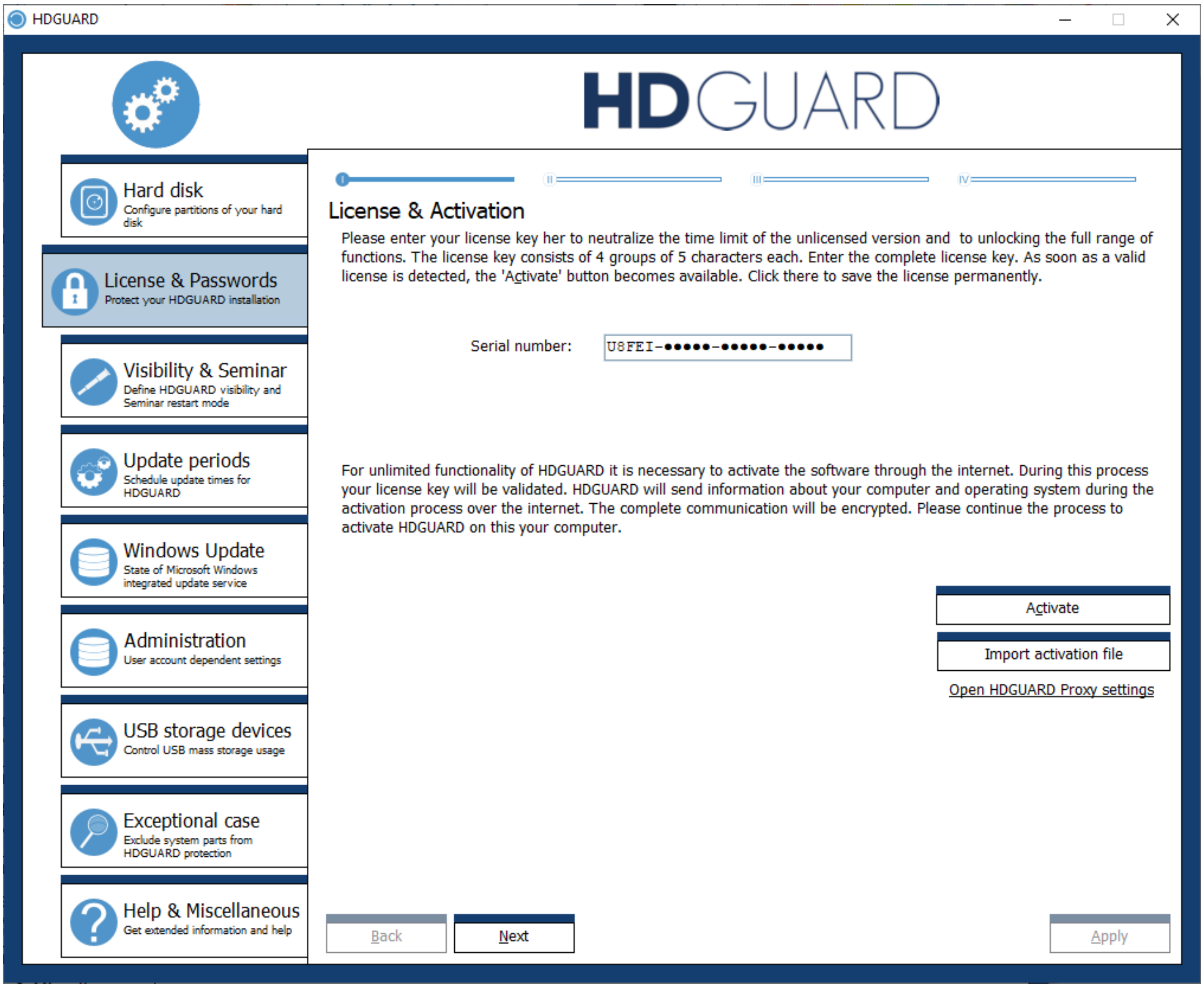
Please note: Some partitions like "System-restore" or "UEFI", only necessary for your system are currently hidden.
Click here to show system partitions

If you want to enable HDGUARD protection for volume C:, just click into the field representing volume C:. 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?
- How many RAM should be reserved in order to speed up the beginning of the SWAP area? Available only for system partitions.

SWAP-RAM option reserves a part of the system's RAM, it decreases boot times significantly.

4.2.2 License and passwords


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
I
II
III
IV
Activate
Import activation file
Open HDGUARD Proxy settings
Back
Next
Apply

License & Activation

Please enter your license key her to neutralize the time limit of the unlicensed version and to unlocking the full range of functions. The license key consists of 4 groups of 5 characters each. Enter the complete license key. As soon as a valid license is detected, the 'Activate' button becomes available. Click there to save the license permanently.

Serial number: U8FEI-●●●●●-●●●●●-●●●●●

For unlimited functionality of HDGUARD it is necessary to activate the software through the internet. During this process your license key will be validated. HDGUARD will send information about your computer and operating system during the activation process over the internet. The complete communication will be encrypted. Please continue the process to activate HDGUARD on this your computer.

Here you can type in your serial number and initiate or repeat the software activation process.

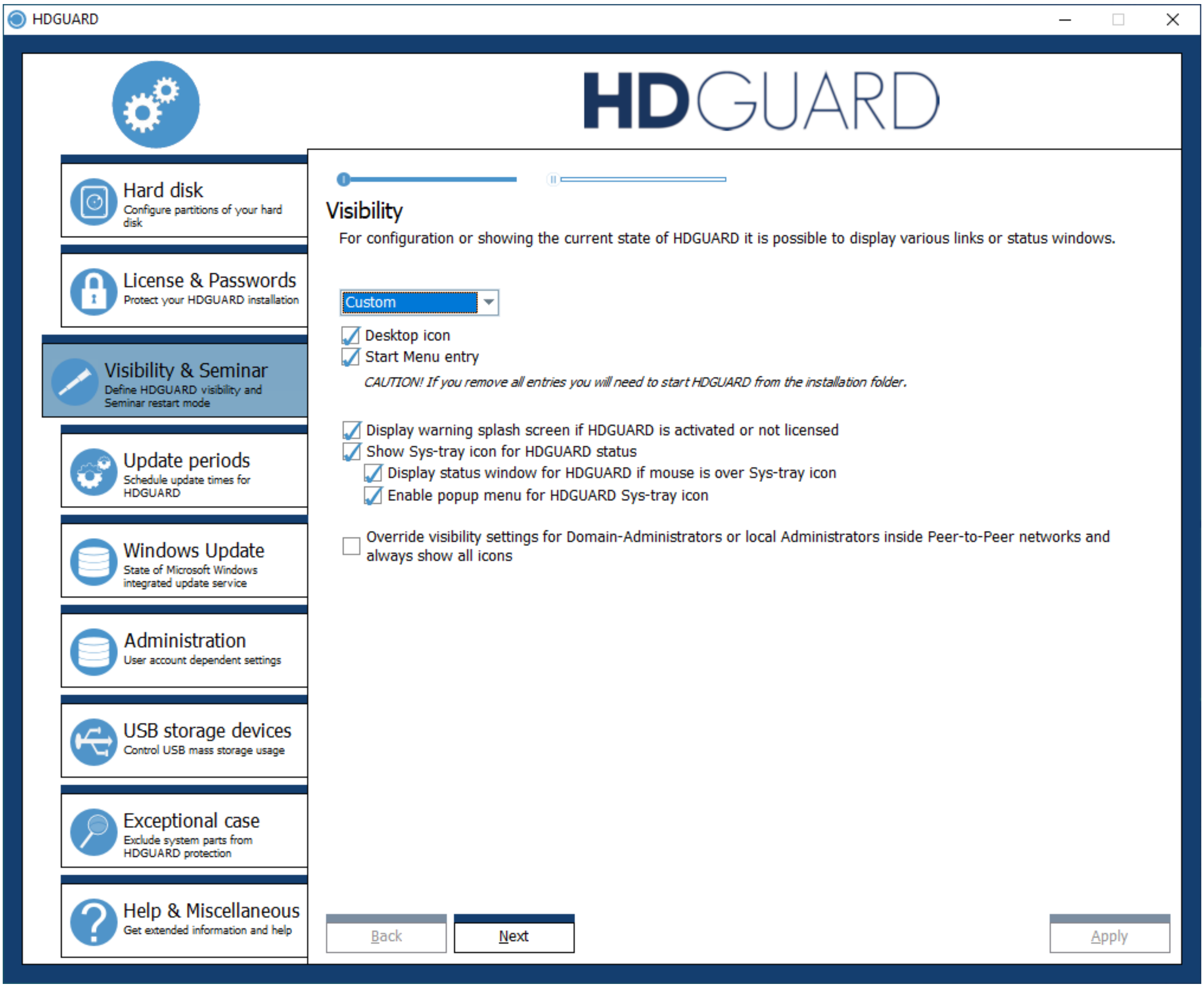
If the local PC cannot establish a connection to the activation server, you can save the request into a file, which you can upload on license-de.ist.com. This step can be done with another PC.
In the second tab (which can be accessed by clicking Next or Back) you can set the HDGUARD password.

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. This feature is available to allow teachers, service personnel or volunteers access to the computer without revealing the password. If a user is authenticated via such *service key* , password changes and the learning further service keys are not possible.

4.2.3 Visibility

In many cases, it is in the interest of the administrator that the presence of HDGUARD remains hidden from the users. The administrator can therefore set the visibility of HDGUARD from "fully visible" to "invisible".


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
Back
Next
Apply

Visibility

For configuration or showing the current state of HDGUARD it is possible to display various links or status windows.

Custom

☑ Desktop icon
☑ Start Menu entry

CAUTION! If you remove all entries you will need to start HDGUARD from the installation folder.

☑ Display warning splash screen if HDGUARD is activated or not licensed
☑ Show Sys-tray icon for HDGUARD status
 ☑ Display status window for HDGUARD if mouse is over Sys-tray icon
 ☑ Enable popup menu for HDGUARD Sys-tray icon

□ Override visibility settings for Domain-Administrators or local Administrators inside Peer-to-Peer networks and always show all icons

Please note that update installations (version updates) of the HDGUARD can partially restore the visibility.

4.2.3.1 Desktop icon

An HDGUARD icon is placed on the desktop. A double-click on this icon starts the HDGUARD program.

4.2.3.2 Start menu entry

Create entries for HDGUARD in the start menu (within "Programs\HDGUARD").

4.2.3.3 Splash screen

A splash screen is displayed when the HDGUARD is active so that the user is informed about the protection of the PC.

4.2.3.4 System tray icon

The system tray (systray) is located on the right hand side of the Windows Start Panel. With the help of the displayed symbol (a sign in the colors blue to red), depending on the utilization, the condition of the protection can be displayed. It is recommended to always display this symbol.

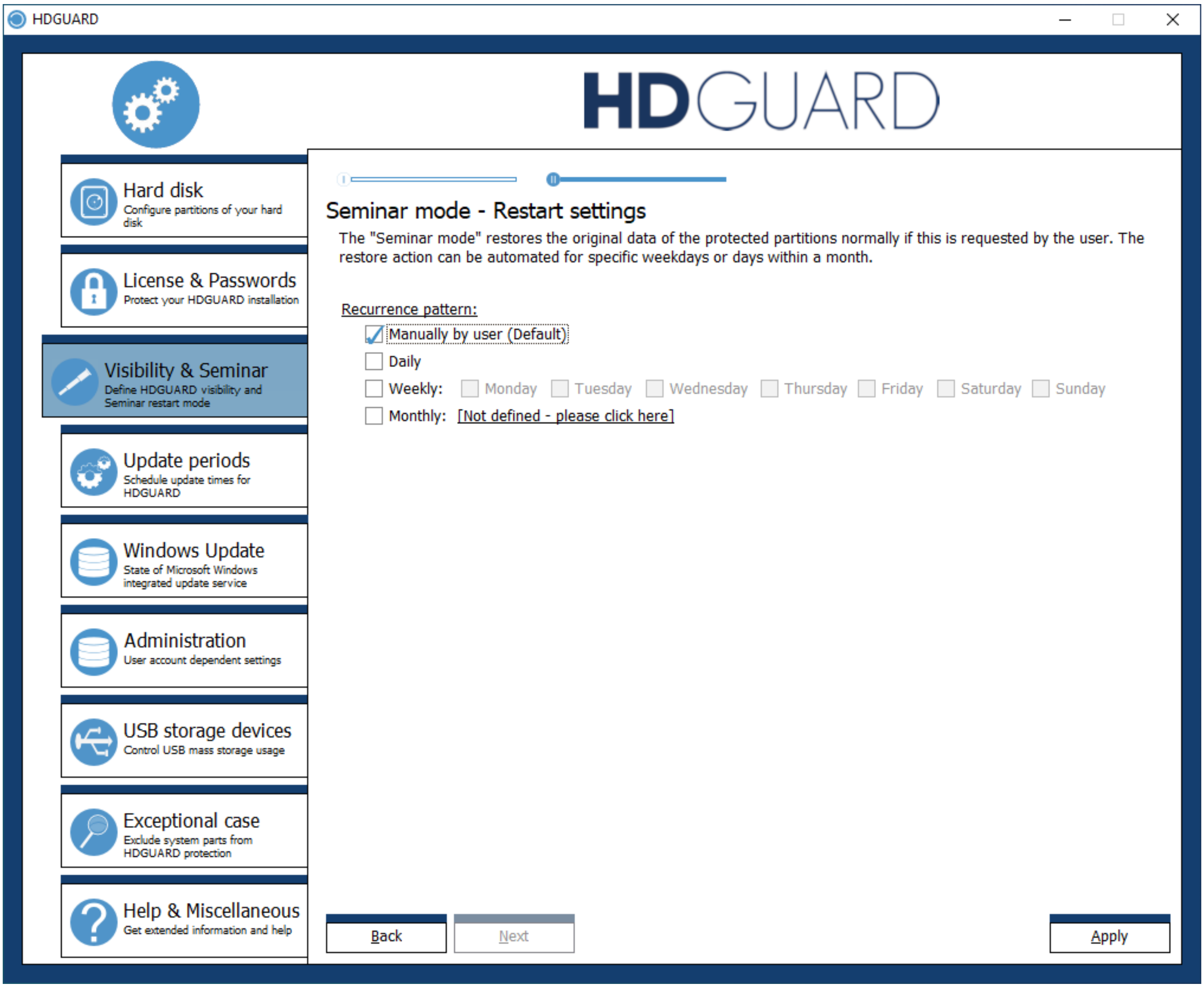
4.2.3.5 Display status window for HDGUARD

When moving the mouse over the tray icon, a status information appears.

4.2.3.6 Seminar Mode - Restart settings

In seminar mode, the user can decide when the protection should be reset. The reset of the seminar mode is done by the user via the tray icon of the HDGUARD when set to Manual and can be protected with a password. Without the password protection, any user can reset the system for the next restart. The password can be stored in Licence and Passwords.

It is also possible to perform the reset automatically on a daily basis, on certain days of the week or on certain days of the month.


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
Back
Next
Apply

Seminar mode - Restart settings

The "Seminar mode" restores the original data of the protected partitions normally if this is requested by the user. The restore action can be automated for specific weekdays or days within a month.

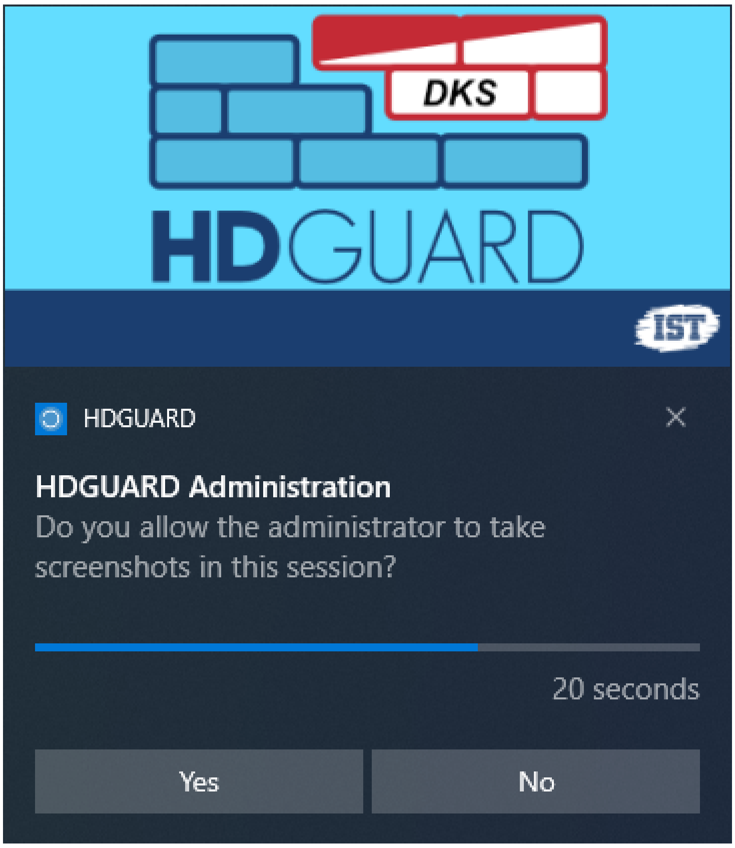
Recurrence pattern:

☑ Manually by user (Default)
☐ Daily
☐ Weekly: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday
☐ Monthly: [Not defined - please click here]

Before the activation of the protection in seminar mode can be used, the reset preferences must be set.

4.2.3.7 Notifications

If a screenshot of a client is requested via the HDGUARD.master, the user must allow this. For a period of 25 seconds, a window is displayed that offers the logged-in user the option of allowing or rejecting the screenshot.



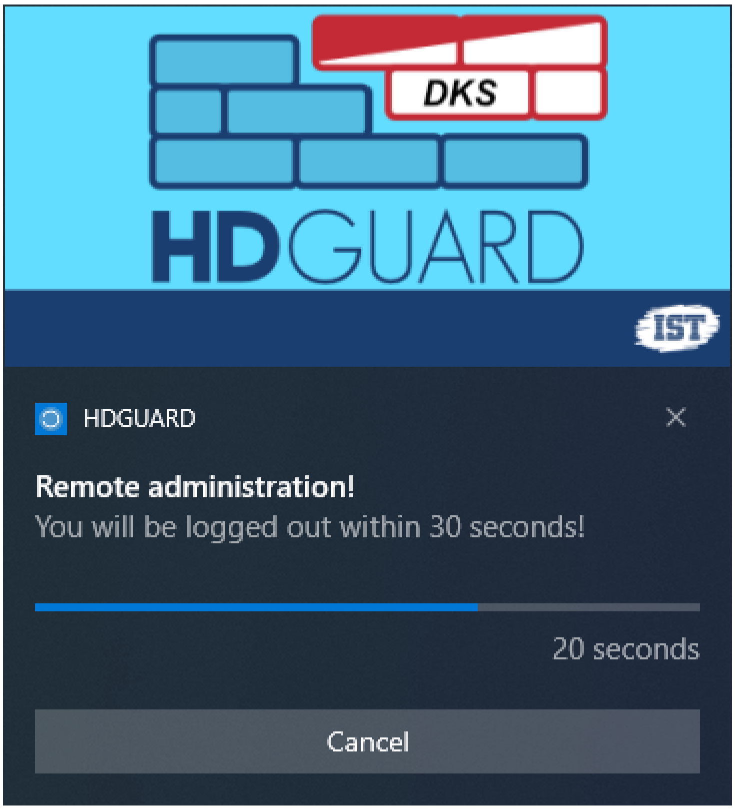
HDGUARD

HDGUARD Administration

Do you allow the administrator to take screenshots in this session?

20 seconds

HDGUARD.master provides the option of remotely logging off users for maintenance purposes. If users are logged in, they can cancel the logout within 30 seconds.

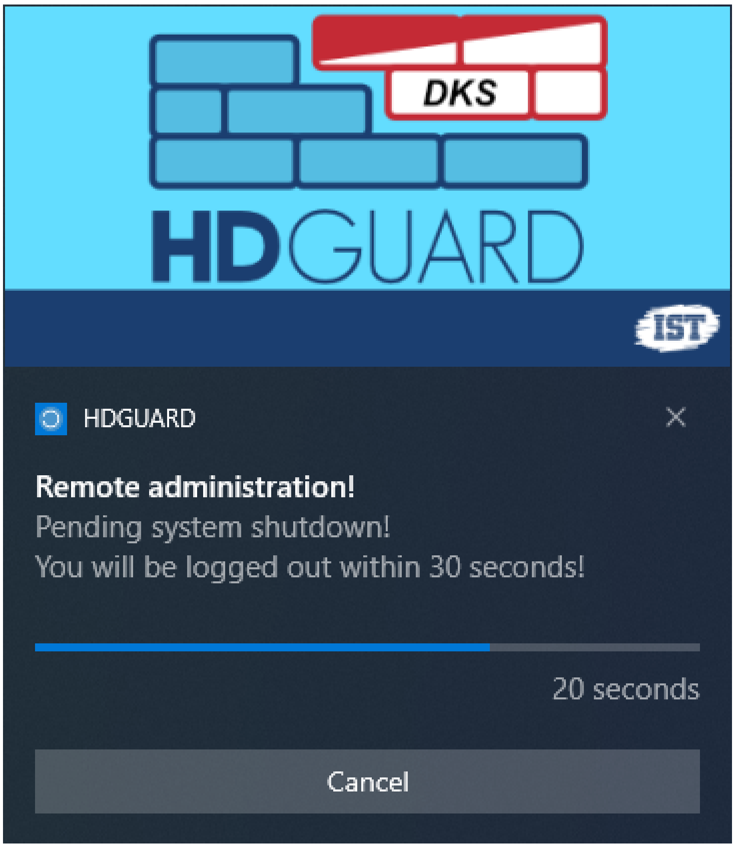


HDGUARD

Remote administration!
You will be logged out within 30 seconds!

20 seconds

HDGUARD.master can be used to shut down PCs remotely. The logged-in user is notified of this and is able to cancel the shutdown within 30 seconds.

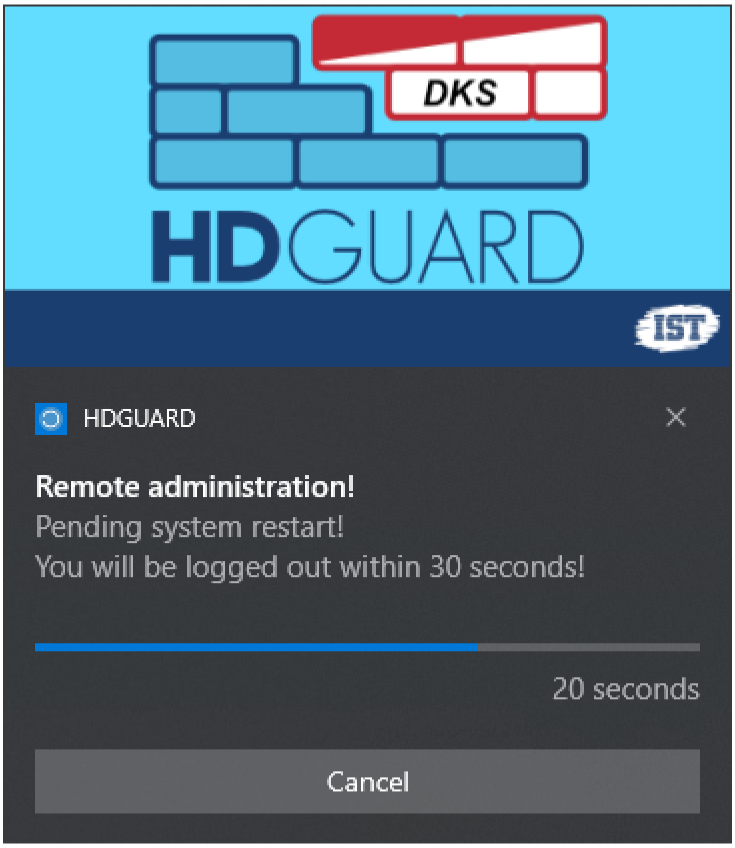


HDGUARD

Remote administration!
Pending system shutdown!
You will be logged out within 30 seconds!

20 seconds

Another notification is displayed if the PC is to be restarted remotely by the HDGUARD.master. Here, as well, the logged-in user has the option of cancelling this process.

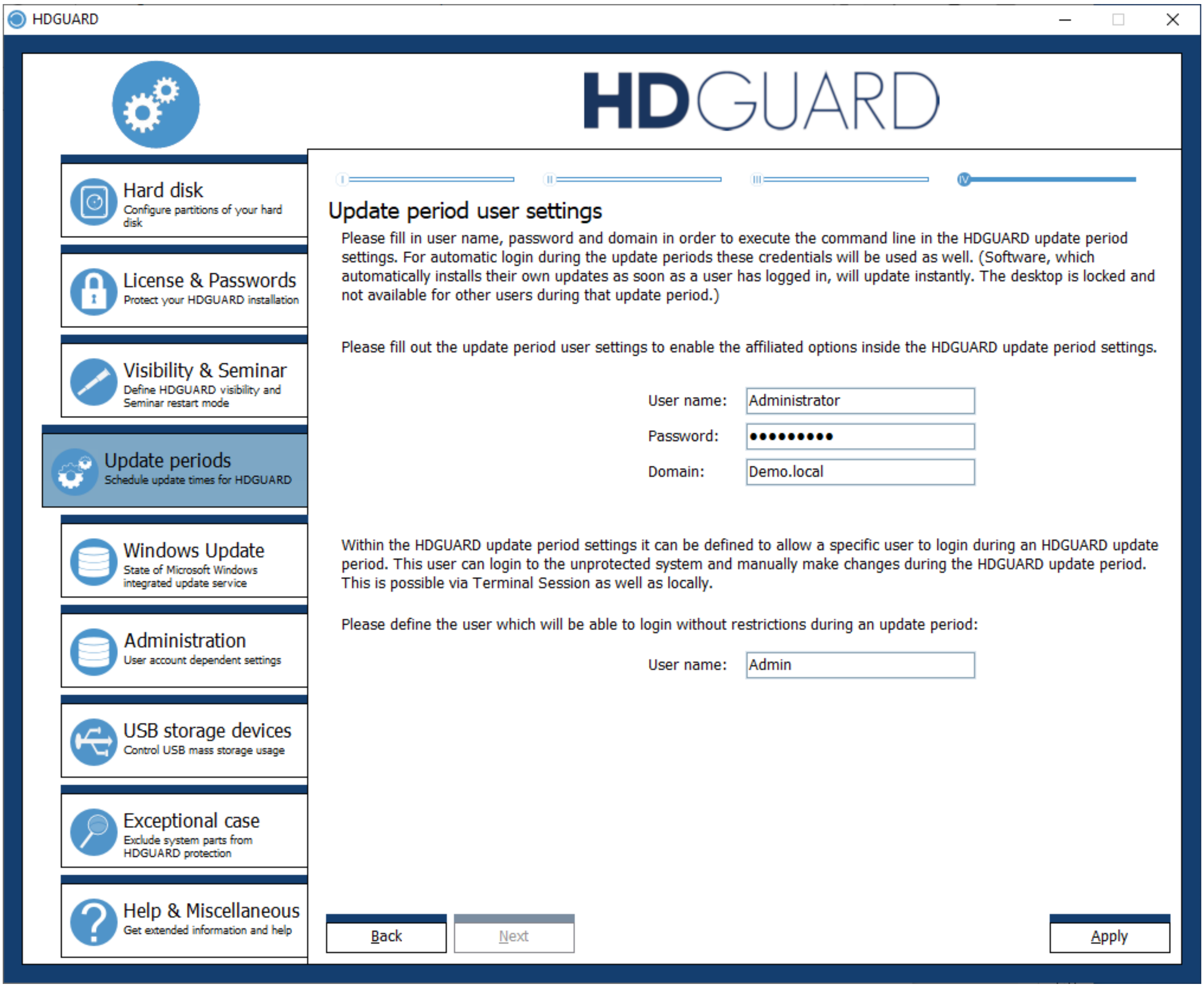


Remote administration!
Pending system restart!
You will be logged out within 30 seconds!

20 seconds

4.2.4 Update periods

To ensure that your operating system and virus scanner are always up to date, you can configure update periods in the HDGUARD.
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.


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
I
II
III
IV
Back
Next
Apply

Update period user settings

Please fill in user name, password and domain in order to execute the command line in the HDGUARD update period settings. For automatic login during the update periods these credentials will be used as well. (Software, which automatically installs their own updates as soon as a user has logged in, will update instantly. The desktop is locked and not available for other users during that update period.)

Please fill out the update period user settings to enable the affiliated options inside the HDGUARD update period settings.

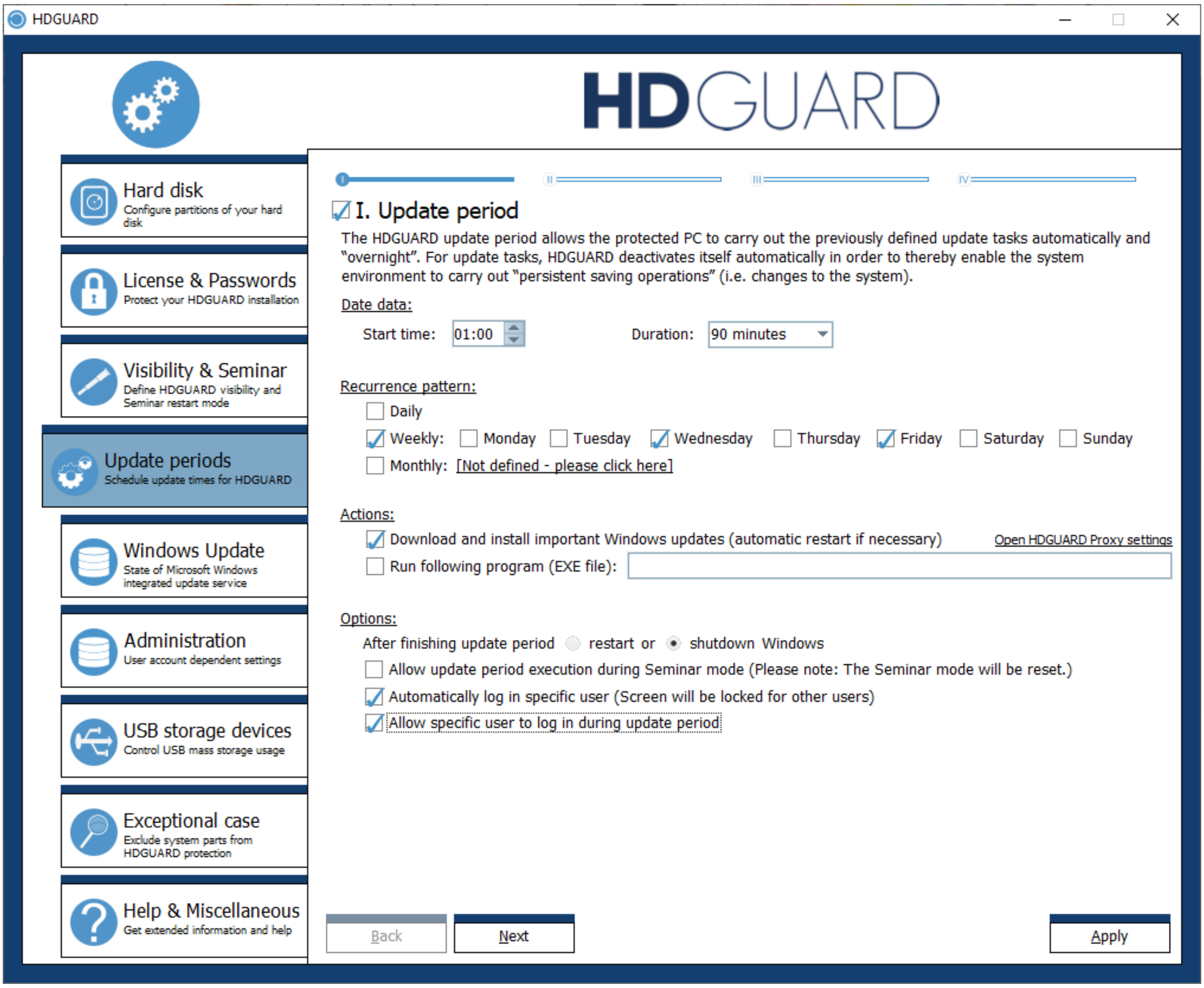
User name: Administrator
Password: •••••••••
Domain: Demo.local

Within the HDGUARD update period settings it can be defined to allow a specific user to login during an HDGUARD update period. This user can login to the unprotected system and manually make changes during the HDGUARD update period. This is possible via Terminal Session as well as locally.

Please define the user which will be able to login without restrictions during an update period:

User name: Admin

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



HDGUARD

HDGUARD

Hard disk
Configure partitions of your hard disk

License & Passwords
Protect your HDGUARD installation

Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode

Update periods
Schedule update times for HDGUARD

Windows Update
State of Microsoft Windows integrated update service

Administration
User account dependent settings

USB storage devices
Control USB mass storage usage

Exceptional case
Exclude system parts from HDGUARD protection

Help & Miscellaneous
Get extended information and help

☑ I. Update period

The HDGUARD update period allows the protected PC to carry out the previously defined update tasks automatically and "overnight". For update tasks, HDGUARD deactivates itself automatically in order to thereby enable the system environment to carry out "persistent saving operations" (i.e. changes to the system).

Date data:

Start time: 01:00 Duration: 90 minutes

Recurrence pattern:

☐ Daily

☑ Weekly: ☐ Monday ☐ Tuesday ☑ Wednesday ☐ Thursday ☑ Friday ☐ Saturday ☐ Sunday

☐ Monthly: [Not defined - please click here]

Actions:

☑ Download and install important Windows updates (automatic restart if necessary) Open HDGUARD Proxy settings

☐ Run following program (EXE file):

Options:

After finishing update period ○ restart or ● shutdown Windows

☐ Allow update period execution during Seminar mode (Please note: The Seminar mode will be reset.)

☑ Automatically log in specific user (Screen will be locked for other users)

☑ Allow specific user to log in during update period

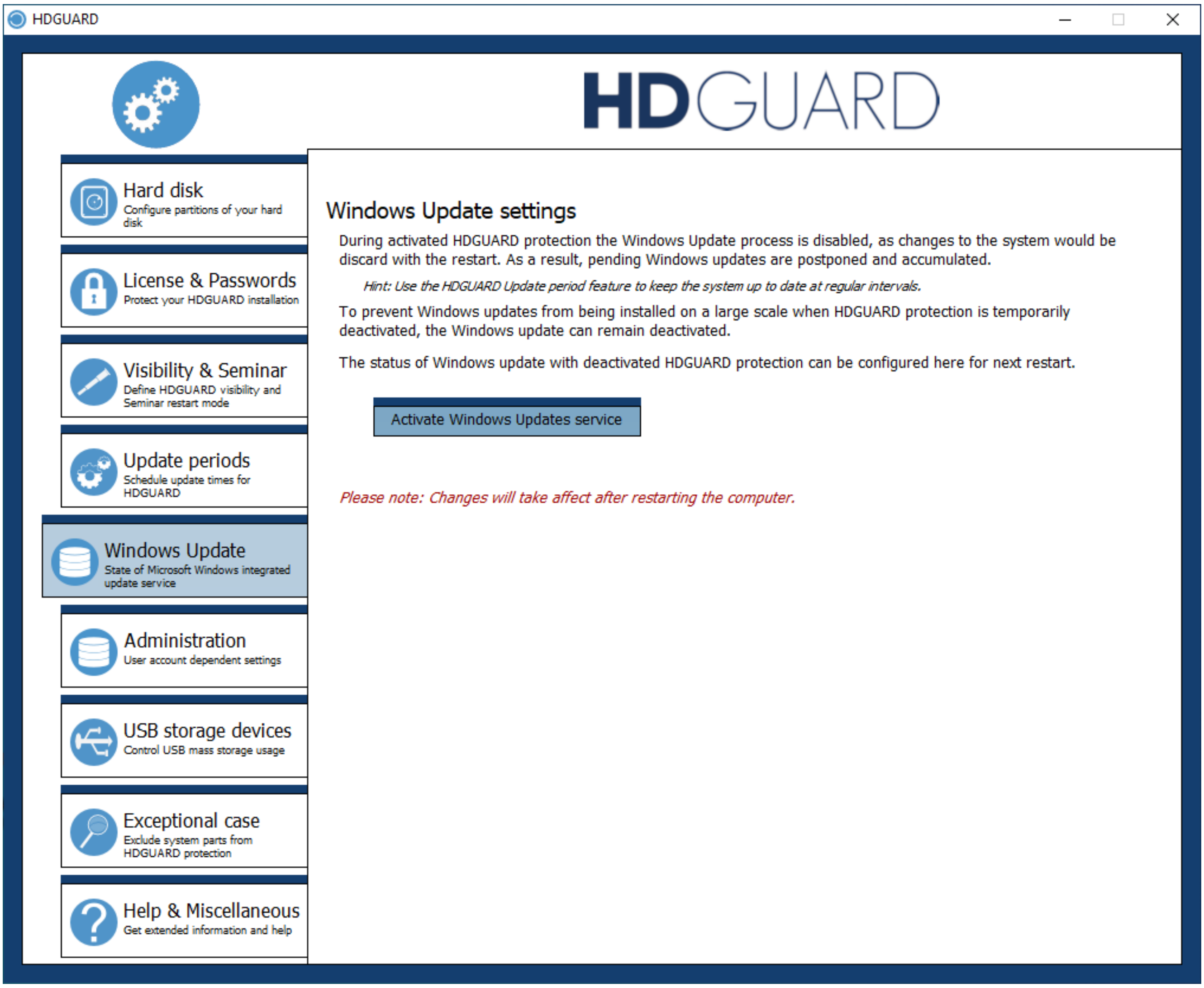
If the installation of Windows updates exceeds the duration of the actual update period, the period will be automatically extended.

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!

In addition to these update periods configured by the user, there are also special, automatic update periods 30.

4.2.5 Windows Update

When protection is activated, the installation of Windows updates is prevented. When protection is deactivated, the update function of the operating system is reactivated. If you wish to modify this standard when deactivating the protection and the update function is to remain deactivated even when the protection is deactivated, this can be changed again in the configuration of the HDGUARD under Windows Update.


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help

Windows Update settings

During activated HDGUARD protection the Windows Update process is disabled, as changes to the system would be discard with the restart. As a result, pending Windows updates are postponed and accumulated.

Hint: Use the HDGUARD Update period feature to keep the system up to date at regular intervals.

To prevent Windows updates from being installed on a large scale when HDGUARD protection is temporarily deactivated, the Windows update can remain deactivated.

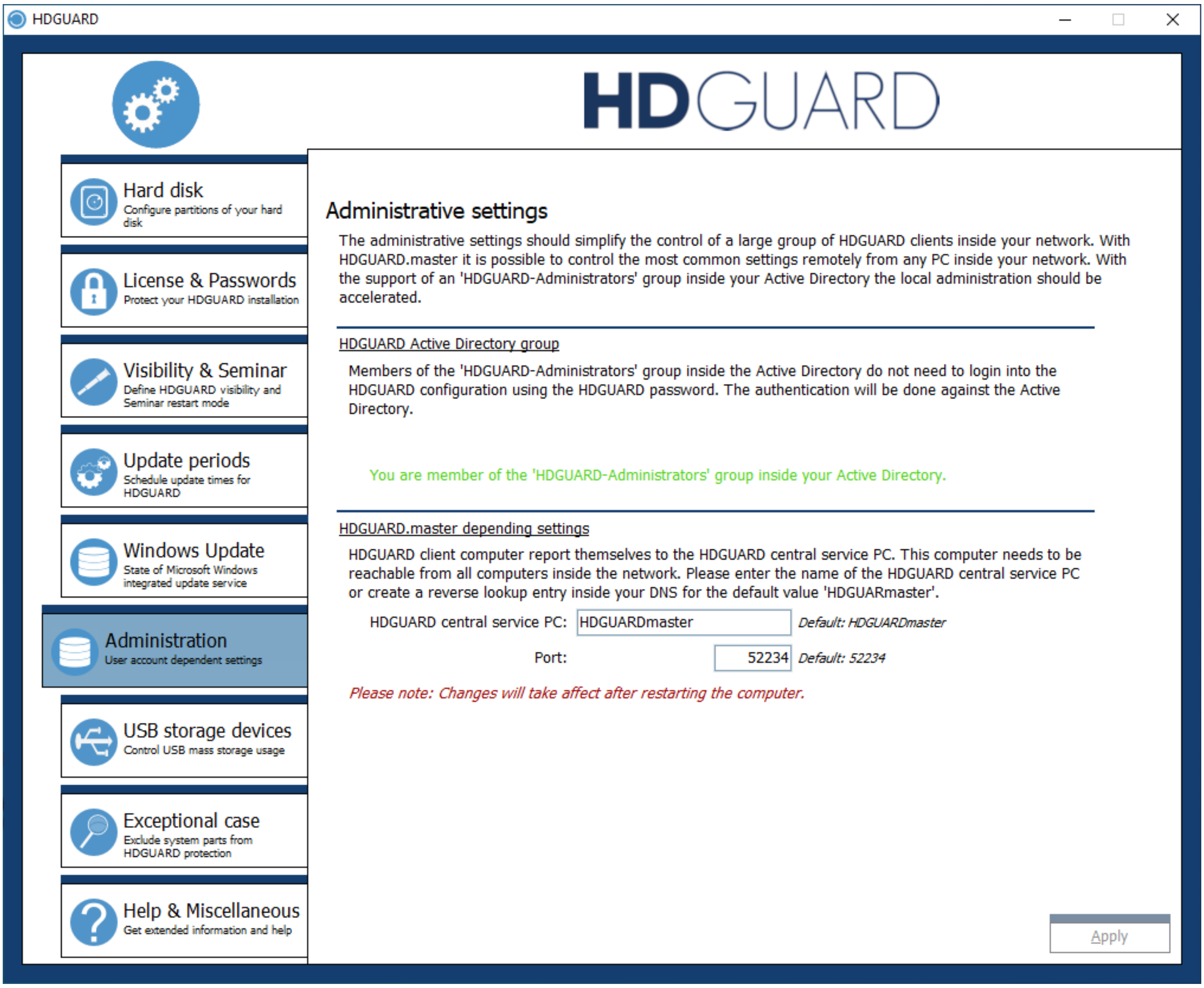
The status of Windows update with deactivated HDGUARD protection can be configured here for next restart.

Please note: Changes will take affect after restarting the computer.

After selecting Activate Windows Updates service and restarting the system, Windows Updates can be installed.

4.2.6 Administration

Members of the AD group "HDGUARD-Administrators" will be able to configure the HDGUARD more easily by not having to enter a password when starting HDGUARD. Setting up the group and assigning members must be done in the domain previously.


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
Apply

Administrative settings

The administrative settings should simplify the control of a large group of HDGUARD clients inside your network. With HDGUARD.master it is possible to control the most common settings remotely from any PC inside your network. With the support of an 'HDGUARD-Administrators' group inside your Active Directory the local administration should be accelerated.

HDGUARD Active Directory group

Members of the 'HDGUARD-Administrators' group inside the Active Directory do not need to login into the HDGUARD configuration using the HDGUARD password. The authentication will be done against the Active Directory.

You are member of the 'HDGUARD-Administrators' group inside your Active Directory.

HDGUARD.master depending settings

HDGUARD client computer report themselves to the HDGUARD central service PC. This computer needs to be reachable from all computers inside the network. Please enter the name of the HDGUARD central service PC or create a reverse lookup entry inside your DNS for the default value 'HDGUARmaster'.

HDGUARD central service PC: HDGUARDmaster *Default: HDGUARDmaster*

Port: 52234 *Default: 52234*

Please note: Changes will take affect after restarting the computer.

AD users from the group "HDGUARD-Administrators" must have local administrator rights, otherwise HDGUARD configuration cannot be started.

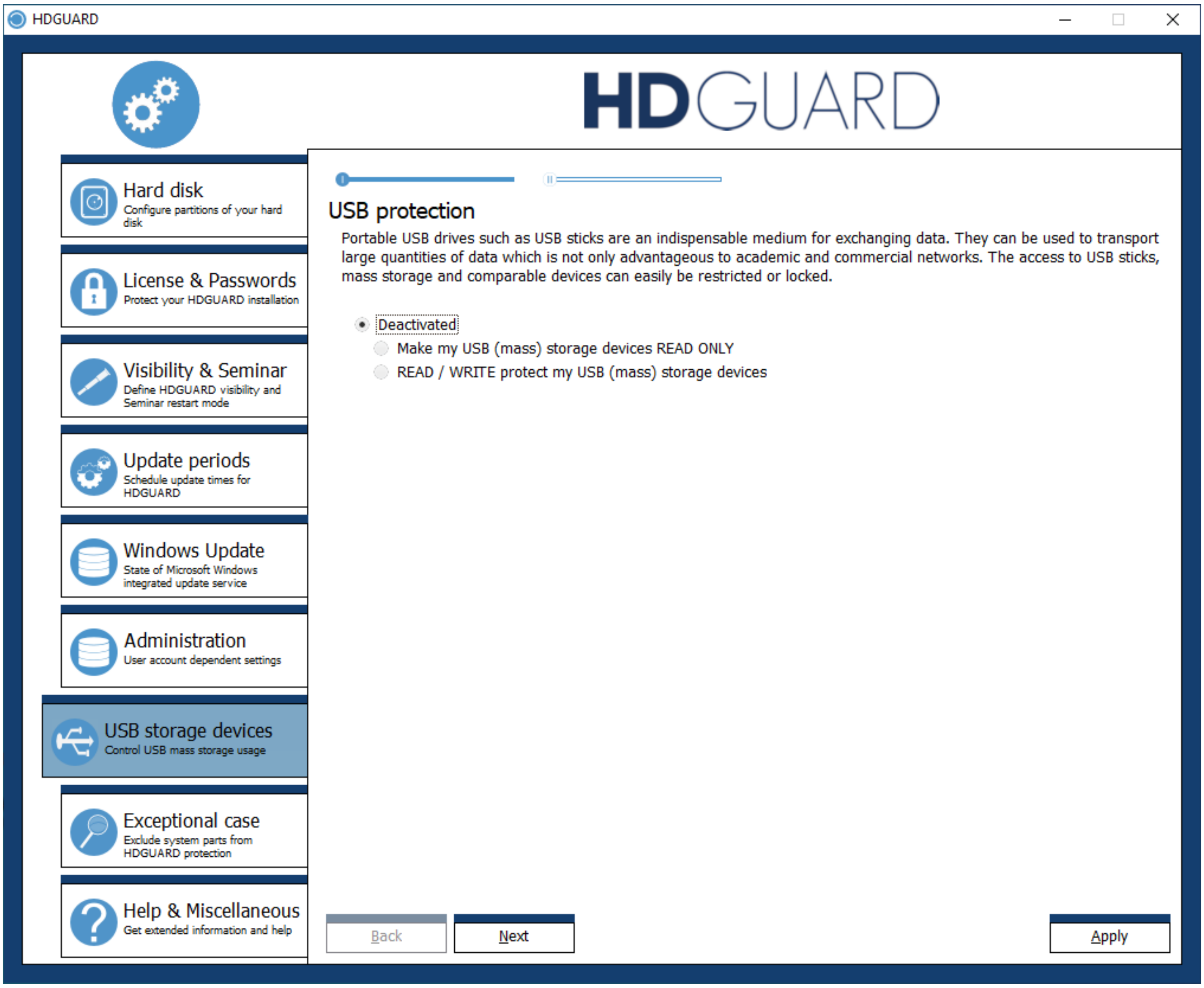
If the protection is deactivated, it is also possible to change the name of the PC on which the central master service is installed.

The port must not be confused or matched with the port for the connections of the HDGUARD.master Remote Proxy service (default 25652)!

4.2.7 USB storage devices

The HDGUARD interface includes a separate handling for USB devices of device class USB mass storage. These can either be provided with write or access protection.

In the second tab you can specify devices that are are always accessible.


HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help
Back
Next
Apply

USB protection

Portable USB drives such as USB sticks are an indispensable medium for exchanging data. They can be used to transport large quantities of data which is not only advantageous to academic and commercial networks. The access to USB sticks, mass storage and comparable devices can easily be restricted or locked.

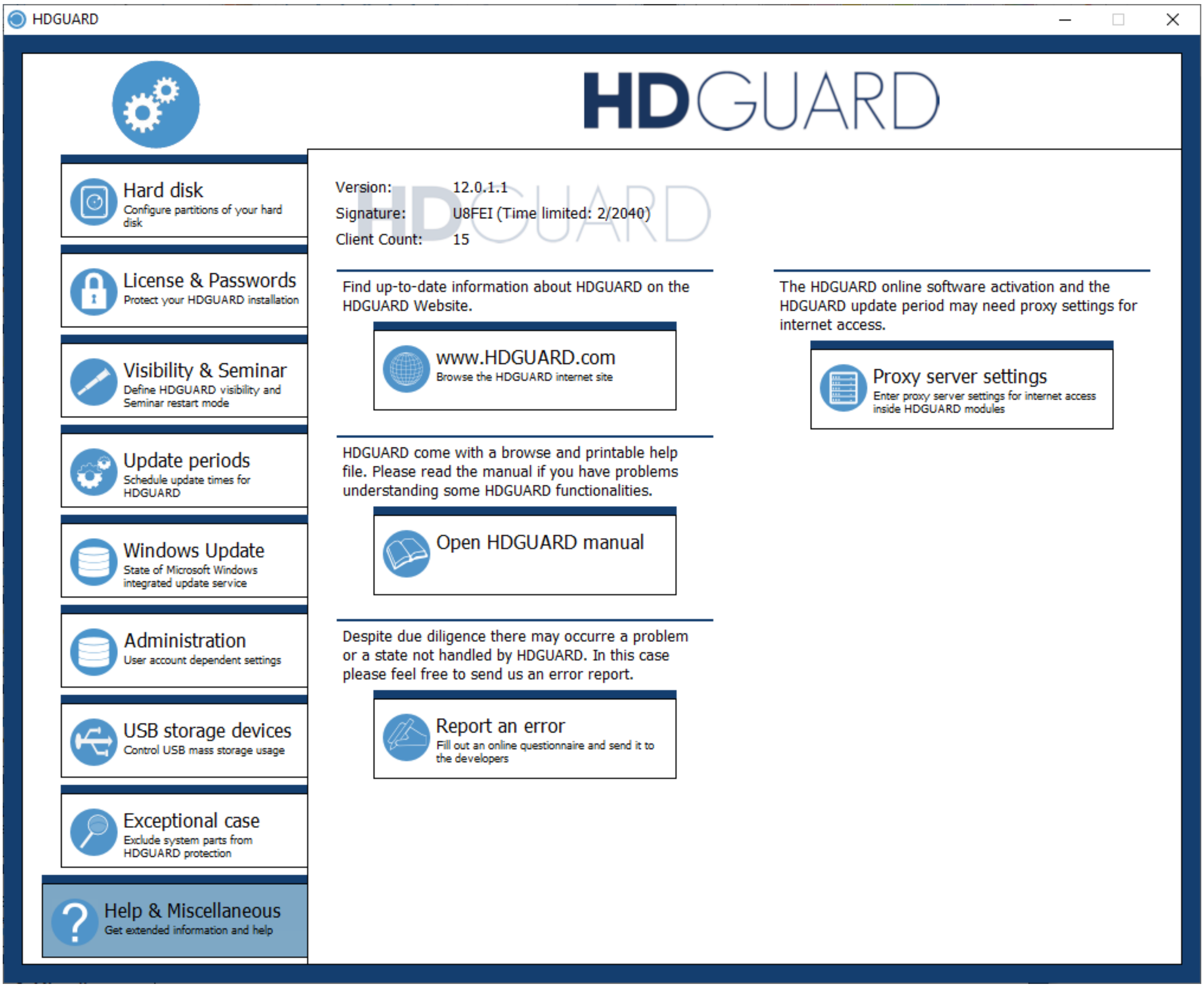
● Deactivated
○ Make my USB (mass) storage devices READ ONLY
○ READ / WRITE protect my USB (mass) storage devices

4.2.8 Exceptional case

The HDGUARD always protects your hard disks by partition. In general, no single files or folders within such a partition can be excluded from HDGUARD protection. The same applies to entries in the system registry, which is also stored in several files on the system partition C: .
The HDGUARD configuration integrates two techniques to realize folder and registry exceptions within narrow bounds. To do this, you need your own NTFS formatted partition, which is not protected by the HDGUARD and which is marked within the configuration.
Folder exceptions are realized as folder redirection. The folder is apparently located on the protected partition, but the NTFS file system redirects access to a hidden folder on the unprotected partition.
Registry exceptions are implemented by periodically backing up the specified registry key to a file on the unprotected partition and restoring the backup at an early system restart. This means that no registry information can be "excluded" which is of any significance for the startup of the operating system. Similarly, it is not possible to capture keys that are not loaded during the operating system startup, such as keys from the hive of the current user "HKCU".

4.2.9 Help & Miscellaneous

This configuration menu item shows version- and license information.



HDGUARD
HDGUARD
Hard disk
Configure partitions of your hard disk
License & Passwords
Protect your HDGUARD installation
Visibility & Seminar
Define HDGUARD visibility and Seminar restart mode
Update periods
Schedule update times for HDGUARD
Windows Update
State of Microsoft Windows integrated update service
Administration
User account dependent settings
USB storage devices
Control USB mass storage usage
Exceptional case
Exclude system parts from HDGUARD protection
Help & Miscellaneous
Get extended information and help

Version: 12.0.1.1
Signature: U8FEI (Time limited: 2/2040)
Client Count: 15

Find up-to-date information about HDGUARD on the HDGUARD Website.

www.HDGUARD.com
Browse the HDGUARD internet site

HDGUARD come with a browse and printable help file. Please read the manual if you have problems understanding some HDGUARD functionalities.

Despite due diligence there may occurre a problem or a state not handled by HDGUARD. In this case please feel free to send us an error report.

Report an error
Fill out an online questionnaire and send it to the developers

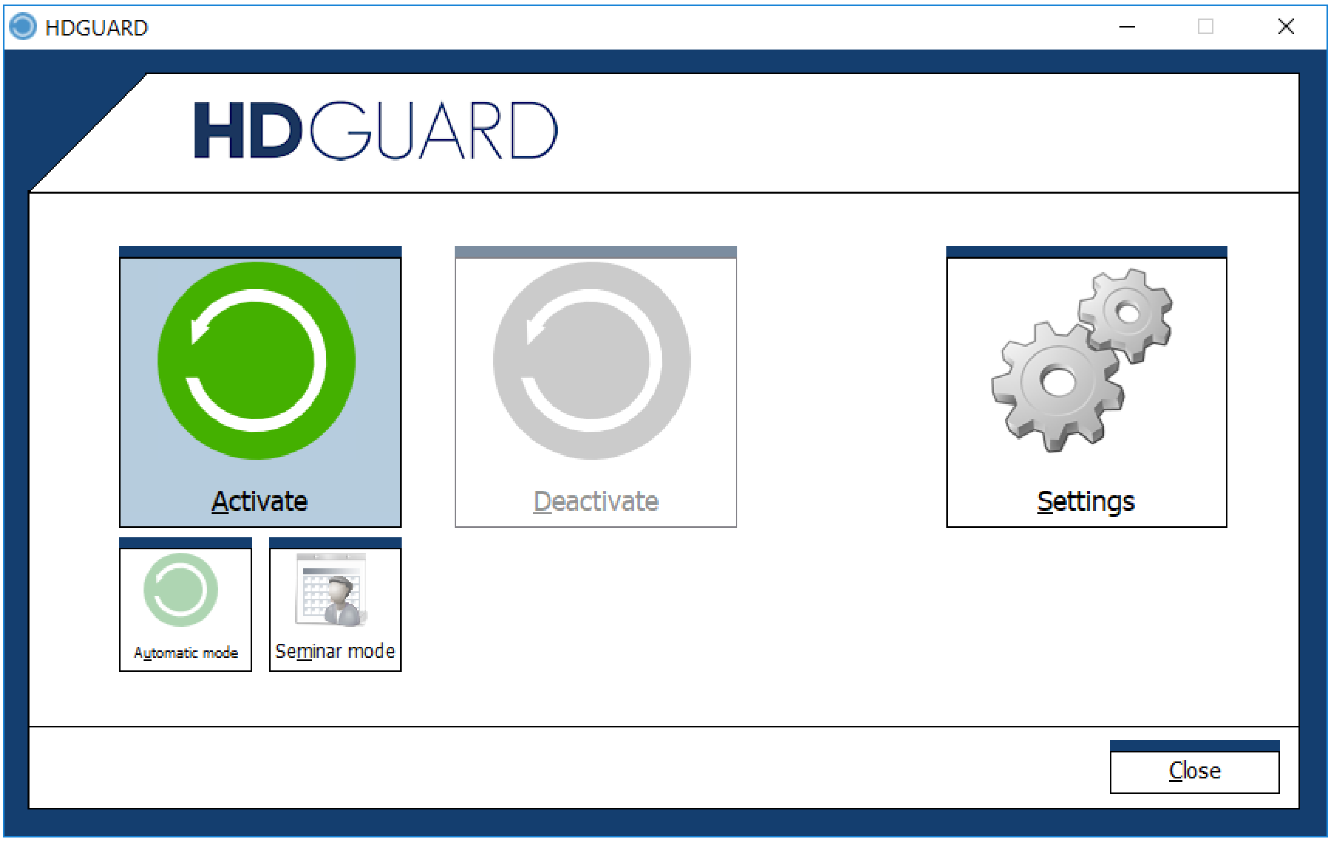
The HDGUARD online software activation and the HDGUARD update period may need proxy settings for internet access.

Proxy server settings
Enter proxy server settings for internet access inside HDGUARD modules

Furthermore, it is possible to open the product web page and give a direct feedback to the development team (Report an error) or to define a proxy connection for the online activation and update periods of HDGUARD.

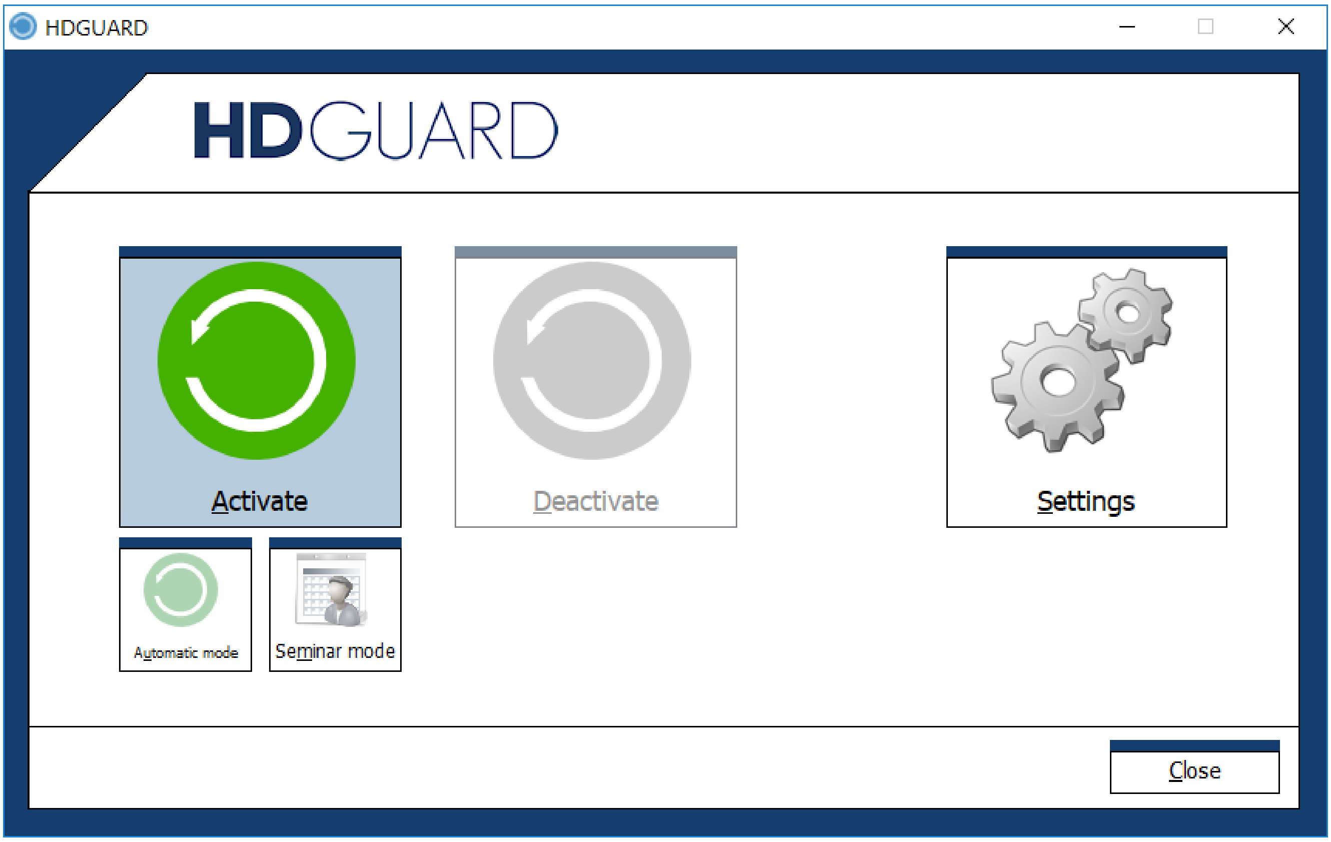
4.3 Main window

After finishing the configuration you are back in the main window. Once the hard disks have been configured, the protection can be activated.



4.3.1 Automatic

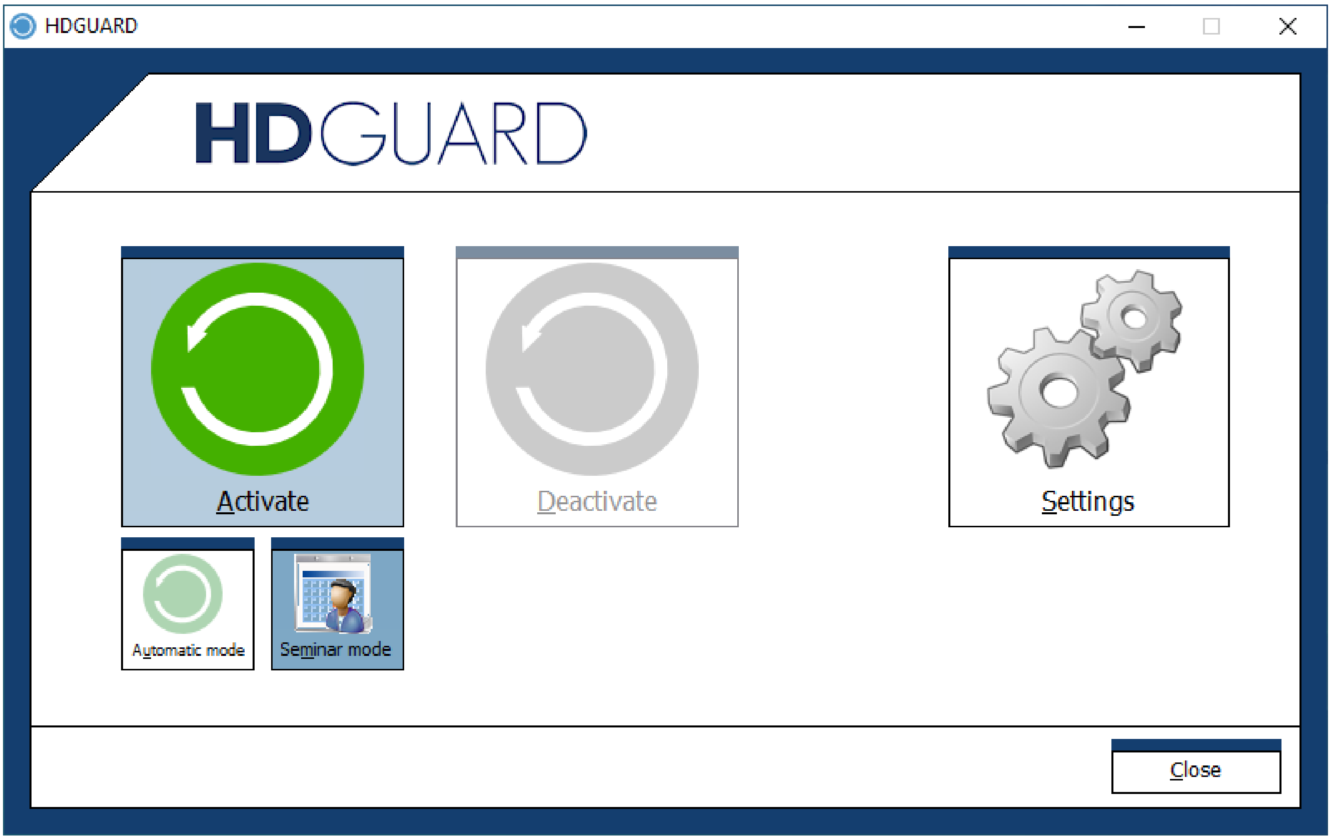
If you select "Activate" - "Automatic Mode", HDGUARD will first make some preparations to protect the system. The computer is then restarted and the protection is activated. Each following restart resets the computer to the state you have set by pressing "Activate".



4.3.2 Seminar mode

If you select "Activate" - "Seminar Mode", the functionality differs from the automatic mode in that way that a restart usually does not return to the original state of the system. The changes from the previous sessions are kept until either

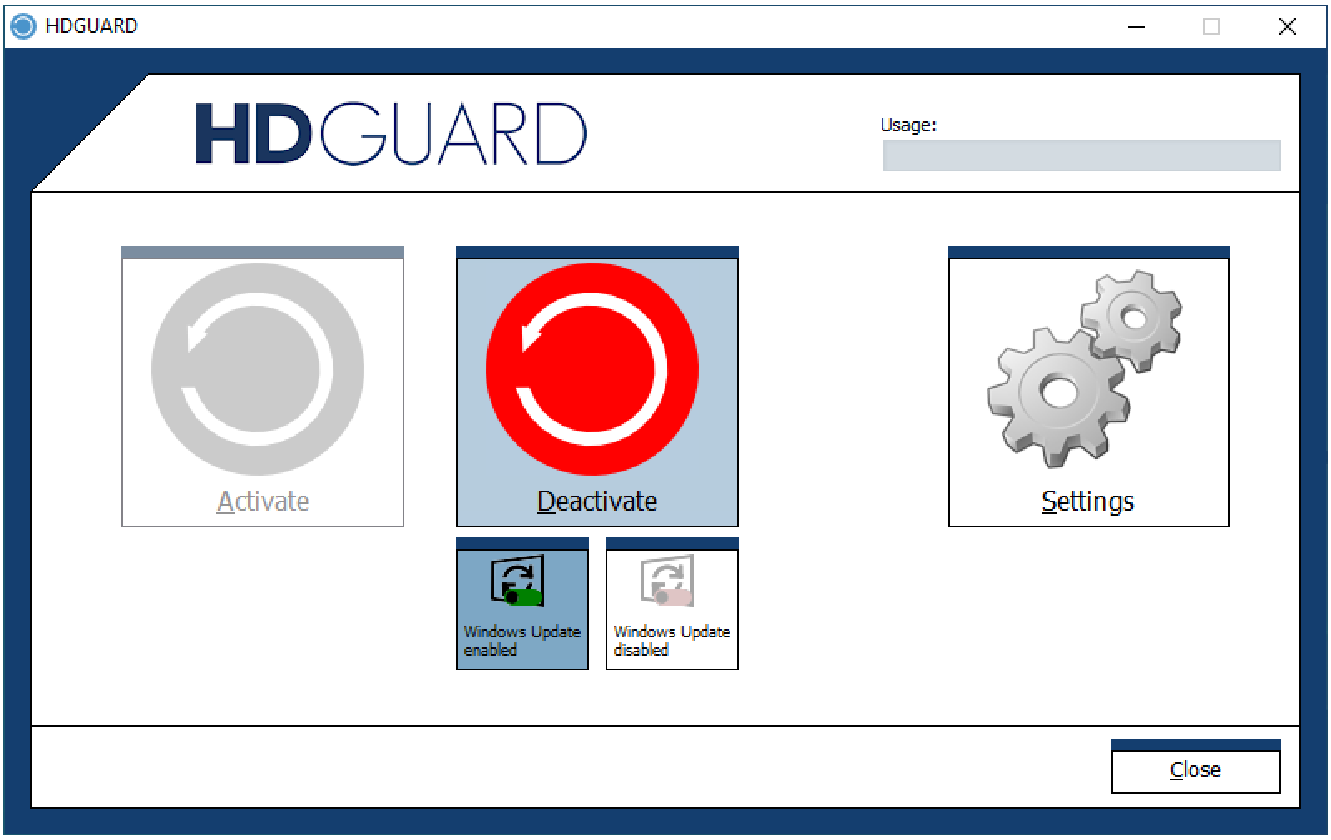
- the storage space in the corresponding HDGUARD SWAP file is exhausted or
- a user selects the "Reset seminar mode" function in the context menu of the HDGUARD System Tray Icon, or
- a configured reset setting is active, or
- an update period begins, whose priority is higher than that of the seminar mode.



Please observe the hints on the reset settings of the seminar mode in the chapter Seminar Mode-Restart Settings 14.

4.3.3 Deactivate

If you select "Deactivate", the HDGUARD protection ends with a restart of the computer. This resets the computer to its original state. Optionally, it is possible to continue to deactivate Windows updates after the restart. By default, Windows updates are executed again after deactivating the protection.



To prevent Windows updates from being installed in large numbers after longer operation in protected mode when protection is deactivated, the update function of the operating system can optionally remain inactive.

We recommend update periods to keep the system up-to-date.

5 Command line operation

To control the HDGUARD automatically via script control or command line, start the executable file HDGcmd.exe out of the program directory with the corresponding parameters.
A command with incorrect or no parameters will display the command line help.

5.1 Commands and 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.
/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 for Windows Updates
                             6 -> Update period 1
                             7 -> Update period 2
                             8 -> 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!
/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.
/ShowWebProxy PWD           :Displays current proxy settings.
/DoWindowsUpdates PWD       :Immediately search for Windows Updates and install
                             them. Reboots into a special update period, if
                             HDGUARD protection is active.
/ShowUMPexclude PWD         :Shows user mode protection exclude list (UMP).
/AddUMPexclude PWD "exe"    :Adds a local executable to UMP list. The file
                             must exist at runtime. Parameter 'exe' must
                             be provided with exe files full path.
/DelUMPexclude PWD "exe"    :Removes a local executable from UMP list.
/DisableWUAUperm PWD        :Leaves automatic Windows Updates disabled when
                             HDGUARD protection ends.
/EnableWUAUperm PWD         :Reenables automatic Windows Updates when HDGUARD
                             protection is deactivated and the system reboots.
```

5.2 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
```

6 Special update periods

HDGUARD recognizes the automatic time change due to the daylight saving time configuration. The first start after a time change happens without HDGUARD protection and without possibility of a user logon. After approx. 2 minutes, the system restarts automatically with active HDGUARD protection.
To prevent boot loops caused by Windows updates with integrated reboot, an automatic update period is started after several reboots without user logon. This also ends after about 2 minutes.

7 Helper functions for cloning

This section describes the setup guide for cloned HDGUARD installations.
If a HDGUARD installation is cloned, the entire hard disk configuration is usually reset. Therefore, it is recommended to clone the HDGUARD without configured hard disks. The first start after cloning is usually detected and an automatic hard disk configuration is initiated.
This can be parameterized with the following registry values.

Create the following registry key: HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\RedirVolumes

Then create a DWORD or QWORD value for each partition to be protected by HDGUARD. Name the value with the drive path (eg. D:). Enter the size of the SWAP file in MByte as value.
The system drive (usually C:) is always configured automatically. Therefore, it only needs to be taken into account if the SWAP file should have a different size from the automatic.
The automatically created start partitions of the newer Windows versions automatically get the property "Read only".

If an HDGUARD password has been set, it must be stored in the key HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\EncPasswords

With the encryption of the "HDGcmd. exe" (see previous section). The value is stored as a simple string with the name "PWD".
If a license key has been entered before cloning, the HDGUARD service finally attempts to establish an Internet connection to the IST software activation server and perform the software activation.

If there is no direct internet connection, you can use the key HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\InternetProxy

Define the settings for your proxy server:

- REG_SZ "value" ProxyNameOrIP "for the address or name of the server.
- REG_DWORD "Value" Port "for the access port.
- If necessary,"REG_SZ" value "LoginName" for the login name of the connection.

- If necessary,"REG_SZ" value "Password" for the associated password.

After automatic configuration, the key HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig is automatically deleted.

8 HDGUARD.master - Connection

In order to be able to administrate individual HDGUARD clients with the optional program HDGUARD.master, a TCP/IP connection to the corresponding PC or server with an installed central HDGUARD.master service must be established. This connection is established by the HDGUARD client.
During the installation of HDGUARD, the (DNS-)Name or IP and, if necessary, a different port of the connection is retrieved and stored in the registry. Without an explicit setting, the following values are used:

- Name: HDGUARDmaster
- Port: 52234

The port must not be confused or matched with the port for the connections of the HDGUARD.master Remote Proxy service (default 25652)!

In larger networks it is recommended to enter an alias (CNAME) within the DNS server on the server where the central HDGUARD.master service is installed.
If this is not possible or if a different port on the computer with the central HDGUARD.master service has to be used, the settings can also be passed to the HDGUARD setup via MSI parameters.

A later modification of the setting is done by changing the registry. The REG_SZ values "Server" and "ServerPort" are stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\IST\HDGUARD

The new values are read in the next time the system is restarted. Do not forget to deactivate the HDGUARD protection before this operation!

9 MSI-Parameters

The following MSI parameters are supported by HDGUARD MSI setup.

- **HDGMASTERNAME** : IP or DNS Name of the system with HDGUARD.master central service installation
- **HDGMASTERPORT** : Port of the HDGUARD.master central service different from the standard (52234)
- **INSTALL_TEACHER** : Boolean value for the installation of the Teacher Console component. INSTALL_TEACHER=yes installes the Teacher Console.
- **HDGLICENSE** : License key without dashes
- **HDGPASSWORD** : HDGUARD password

Be careful with the parameters, especially when passing the password, that the command line treats certain characters as control and separator characters and does not pass them directly to the calling program.

For an unattended installation, the command line would look like this:

```
msiexec /i HDGUARD11_64.msi /qn HDGMASTERNAME=MyHDGUARDmasterPC HDGMASTERPORT=50000 INSTALL_TEACHER=yes
```

10 Teacher console

The HDGUARD Teacher Console provides certain functionalities of the HDGUARD. master on a teacher's desk within a HDGUARD.master room. You can wake up and shut down HDGUARD clients, lock and unlock the screen, audio, Internet or printers.
Please read the corresponding section in the manual of the HDGUARD.master.