# HDGUARD 11 Referenzhandbuch

# HDGUARD 11 Referenzhandbuch



Herausgeber:

*IST Deutschland GmbH*
*Bergstraße 23*
*23843 Neritz*
*Tel: +49 4531 8804-40*
*Fax: +49 4531 8804-44*
*Email: info@rdt.de*
*Web: www.rdt.de*

*IST Deutschland GmbH*
*HRB 1408, OD Lübeck*
*Geschäftsführer: David Baunsgaard*

# 1 Einführung

## 1.1 HDGUARD

HDGUARD schützt Ihre Festplatten vor dauerhaften Veränderungen. Nach einem Neustart des Rechners wird automatisch der gewünschte Originalzustand wiederhergestellt. Selbst wenn die Anwender Dateien verändern oder löschen, hat dies keinen dauerhaften Effekt. Die hohe Betriebssicherheit der geschützten PCs entlastet verantwortliche IT-Mitarbeiter und sorgt für eine ungewöhnlich hohe Langzeitstabilität - sogar bei PCs in öffentlichen Einrichtungen!
Erzielt wird die hohe Betriebssicherheit dadurch, dass HDGUARD alle Veränderungen an den konfigurierten Partitionen entweder unterbindet oder in HDGUARD SWAP Dateien umleitet. Zur Laufzeit des Betriebssystems können alle Funktionen ohne Einschränkungen genutzt werden und der Anwender erkennt keinen Unterschied im Vergleich zu herkömmlichen, ungeschützten PCs. Sobald der PC neugestartet wird, verwirft HDGUARD alle Änderungen. Hierfür wird nur ein Bruchteil einer Sekunde benötigt, egal wie umfangreich die Änderungen waren.
Die Funktionalität des HDGUARD wird abgerundet durch einen wirkungsvollen USB Schutz, der die Nutzung von USB-Laufwerken einschränkt. Zusätzlich stellen eine Vielzahl nützlicher Optionen sicher, dass sich die Software sehr gut in bestehende IT-Konzepte integrieren lässt. Damit eignet sich HDGUARD für praktisch jeden Einsatzbereich.
Über die klassischen Schutzfunktionen hinaus wurden einige sehr nützliche didaktische Funktionen zur HDGUARD Produktfamilie hinzugefügt. Weitere Informationen dazu finden Sie im Handbuch für das Produkt HDGUARD.master.
HDGUARD ist eine reine Softwarelösung. Es sind keine Hardwareeingriffe an den geschützten Systemen erforderlich. Durch Verzicht auf PC-Karten oder Dongle fügt sich HDGUARD perfekt in neue als auch in bestehende Systeme ein.

## 1.2 HDGUARD.master

HDGUARD.master zentralisiert die Steuerung und Überwachung der HDGUARD geschützten Rechner in Ihrem Netzwerk. Deaktivieren Sie gezielt einzelne Rechner oder ganze Räume. Überwachen Sie automatisch den Schutz Ihrer Rechner und lassen Sie Sicherheitswarnungen erscheinen, wenn ein Rechner ungeschützt hochgefahren ist.
HDGUARD.master ist die perfekte Ergänzung für alle Netzwerke, in denen HDGUARD geschützte PCs zum Einsatz kommen.

# 2 Installation

Fertigen Sie Sicherheitskopien aller wichtigen Daten bzw. des gesamten Systems an. Durch Fehlbedienung, fehlerhafte Installation, außerplanmäßige Unterbrechung der Installation oder Fehlkonfiguration können Daten beschädigt werden oder verloren gehen. Die Firma IST Deutschland GmbH und ihre Partner haften nicht für eventuelle Datenverluste und deren Folgen.

Wenn HDGUARD und (ggf. Teile des) HDGUARD.master auf einem System installiert werden sollen, muss HDGUARD.master zuerst installiert werden.

## 2.1 Art des HDGUARD Schutzes und Einschränkungen

HDGUARD schützt die Daten auf der Festplatte grundsätzlich per Partition. Das heißt, dass alle Änderungen an Registryeinträgen und an Dateien auf dem Systemlaufwerk *C:* auf jeden Fall durch einen Neustart zurückgesetzt werden. HDGUARD bietet für bestimmte Szenarien Hilfsfunktionen an, mit denen sich diese Einschränkungen abmildern lassen. Es wird empfohlen, Updatezeiträume 13 zu nutzen, um bei zeitweise deaktiviertem HDGUARD Schutz Updates etc. einspielen zu können. In selteneren Fällen können auch Ausnahmen 16 verwendet werden. Dazu ist eine zusätzliche Partition auf der Systemfestplatte notwendig, die Sie mit Hilfe der Windows Datenträgerverwaltung auch nachträglich anlegen können.

Der Windows Update Dienst ist zur Laufzeit des HDGUARD Schutzes deaktiviert. Betriebssystem- und Defender-Updates können nur bei deaktiviertem Schutz installiert werden. Außerdem ist die Funktionalität des Microsoft App-Stores eingeschränkt, wenn der HDGUARD Schtz aktiv ist.

## 2.2 Systemvoraussetzungen

### 2.2.1 Hardware

Handelsüblicher PC mit Intel-X86 oder AMD64 Prozessorarchitektur und mindestens 2 GB RAM und 50 GB Festplatte, SHDD oder SSD.

RAID-Systeme und Installationen in virtuelle Maschinen werden nicht unterstützt.

### 2.2.2 Betriebssysteme

Microsoft Windows 10, Windows 8, Windows 8.1, Windows 7
Microsoft Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Jeweils für die Architektur X86 und AMD64(x64)

### 2.2.3 Festplatteneinrichtung

MBR oder GPT mit primären und sekundären Partitionen.
Von HDGUARD berücksichtigte Volumes mussen mit NTFS oder FAT32 formatiert sein.

Partitionszusammenführungen wie dynamische Datenträger werden nicht unterstützt.

### 2.2.4 Freier Speicher

Mindestens 4 GB freier, zusammenhängender Speicher auf dem Systemlaufwerk *C:* , empfohlen mindestens 20 GB freier, zusammenhängender Speicher auf dem Systemlaufwerk *C:* .

## 2.3 Installation über die Benutzeroberfläche

Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
Starten Sie nun auf einer 32-Bit Windows Installation `HDGUARD11_32.msi` und auf einer 64-Bit Windows Installation `HDGUARD11_64.msi` . Sie erhalten die aktuellen Installationsquellen im Internet unter www.rdt.de. Die Lehrerkonsole 23 funktioniert nur zusammen mit dem HDGUARD.master. Sie sollte nur an den Arbeitsstationen mitinstalliert werden, an denen auch Dozenten arbeiten. Sobald HDGUARD vollständig installiert ist, erscheint ein Dialog zum Neustarten des Rechners.

Der Neustart des Rechners nach der Installation ist zwingend erforderlich, bevor weitere Aktionen durchgeführt werden.

## 2.4 Installation in einen Klon-Master

Richten Sie das Betriebssystem und alle Anwendungen ein.
Installieren Sie nun auf einer 32-Bit Windows Version `HDGUARD11_32.msi` und auf einer 64-Bit Windows Version `HDGUARD11_64.msi` . Sie erhalten die aktuellen Installationsquellen im Internet unter www.rdt.de.
Führen Sie nun die Konfiguration in der HDGUARD Oberfläche durch. Dabei dürfen Sie noch keine Festplattenpartitionen einrichten. Nach dem Klonen wird eine automatische Festplatteneinrichtung durchgeführt. Die Softwareaktivierung muss nach dem Klonen erfolgen. Dazu stehen Einrichtungshilfen bereit. Lesen Sie dazu den Abschnitt Hilfsfunktionen beim Klonen 21.

HDGUARD darf nicht mit bereits konfigurierten Festplatten geklont werden!

Fertigen Sie nun von diesem Zustand das Rechnerimage an.
Für das weitere Einrichten der Klone stehen Ihnen außerdem die Kommandozeilensteuerung 19 `HDGcmd.exe` und ggf. das Programm HDGUARD.master zur Verfügung.

## 2.5 Installation und Einrichtung eines Multibootsystems

HDGUARD unterstützt Multibootsysteme mit dem Windows Bootmanager.
Für die Einrichtung eines solchen Systems gehen Sie wie folgt vor:
Legen Sie zunächst die Setup DVD der höchsten zu installierenden Windows Version ein und starten Sie das Setup. Klicken Sie im Partitionierer zunächst auf Laufwerkoptionen (erweitert) und löschen Sie alle vorhandenen Partitionen auf der Startfestplatte. Klicken Sie nun auf Neu und geben Sie die Größe für die Systempartition *C:* ein, die für diese Windowsversion benutzt werden soll. Erstellen Sie anschließend mit Hilfe dieses Partitionierers auch die anderen Partitionen für die weiteren zu installierenden Windowsversionen und ggf. eine zusätzliche für ungeschützte Daten.
Wenn Sie mit dem Partitionierer fertig sind, klicken Sie nicht auf Weiter, sondern nehmen Sie die DVD aus dem Laufwerk und legen die Setup DVD oder CD der ältesten Windowsversion ein, die Sie in das Multibootsystem integrieren wollen, und starten Sie das System neu. Installieren Sie nun die Windowssysteme von der ältesten bis zur neuesten Windowsversion jeweils in die vorgesehene Partition. Es können auch Linuxsysteme in das Multibootsystem aufgenommen werden. Diese müssen ihren Bootcode in dem Startsektor ihrer jeweiligen Bootpartition ablegen und in den Windows Bootmanager eingetragen werden. (Anleitungen dazu finden sich im Internet.)
Mit diesem Vorgehen stellen Sie sicher, dass der aktuelle Windows Bootmanager verwendet wird und keine Reparatur von bereits bestehenden Systemen erfolgen muss oder gar externe Tools eingesetzt werden müssen. Wenn Sie die einzelnen Windowssysteme installiert und eingerichtet haben, installieren Sie auf jedem Windowssystem den HDGUARD. Führen Sie anschließend die Konfiguration des HDGUARD auf einem Windowssystem aus. Dabei ist zu beachten, dass jede Partition, die eine Windowsinstallation enthält, auf den Modus „zu schützen“ und ggf. vorhandene, versteckte Startpartitionen auf „nur Lesen“ oder „kein Zugriff“ gestellt werden müssen.
Diese Konfiguration des HDGUARD Schutzes gilt für alle Windowsinstallationen auf dem Multibootsystem, sodass sie nur einmal durchgeführt werden muss. Gleiches gilt für die Softwareaktivierung 8.
Nach Abschluss der Konfiguration des HDGUARD starten Sie nun beginnend mit der ältesten installierten Windowsversion auf allen Installationen jeweils die HDGUARD Oberfläche und drücken Sie auf

*Aktivieren* und *Automatik* bzw. *Seminar Modus* . Bei der Nachfrage zum Multibootsystem wählen Sie jedoch *Nein* aus. Erst wenn Sie bei der neuesten Windowsversion angekommen sind, wählen Sie *Ja* aus. Damit ist sichergestellt, dass alle Windows Installationen auf den HDGUARD Schutz vorbereitet sind.

# 3 Lizenzierung und Testzeitraum

## 3.1 Testzeitraum

Nach der Installation des HDGUARD haben Sie 30 Tage Zeit, die Software ohne Eingabe einer Seriennummer zu testen. Innerhalb dieses Zeitraums stehen Ihnen bis auf den Kennwortschutz 11 und die Anpassung der Sichtbarkeit 12 alle Funktionen zur Verfügung.

## 3.2 Lizenzierung

Nach der Eingabe einer gültigen Seriennummer 11 erhalten Sie die volle Funktionalität bis maximal 60 Tage nach der Installation.

## 3.3 Softwareaktivierung

Die uneingeschränkte Funktionalität steht Ihnen erst nach einer Registrierung der einzelnen Installation bei IST Deutschland GmbH zur Verfügung (Softwareaktivierung). Dabei wird ein Datenpaket bestehend aus der HDGUARD Seriennummer und der Identifizierung der Hardware an einen Server von IST Deutschland GmbH geschickt. Mit der daraus generierten Antwort, ist die HDGUARD Installation i.d.R dauerhaft lauffähig. Diese Antwort enthält nicht nur die Information zur eigentlichen Freischaltung sondern auch ggf. aktualisierte Lizenzinformationen.
Dieser Datenaustausch geschieht bei direkter (oder Proxy-) Internetverbindung über die HDGUARD Benutzeroberfläche oder über das HDGUARD Kommandozeilentool HDGcmd. Liegt keine Internetverbindung vor, können beide Programme alternativ eine Anfragedatei erstellen, die auf der Internetseite activation.rdt.de/HDGUARD entgegengenommen wird. Die Seite generiert eine rechnerspezifische Antwortdatei, die von den beiden oben genannten Programmen entgegen genommen wird. Die Verbindung bei der automatischen sowie manuellen Aktivierung von HDGUARD ist nach aktuellem Stand der Technik verschlüsselt.

Die Softwareaktivierung kann im Gegensatz zu der Aktivierung von Microsoft Windows oder Microsoft Office am einzelnen PC beliebig oft durchgeführt werden, ohne dass die entsprechende Lizenz zusätzlich „verbraucht“ wird. Auch eine wiederholte Installation von HDGUARD auf demselben Rechner mit erneuter Softwareaktivierung „verbraucht“ die entsprechende Lizenz nicht weiter, solange die Hardware nicht geändert wird.

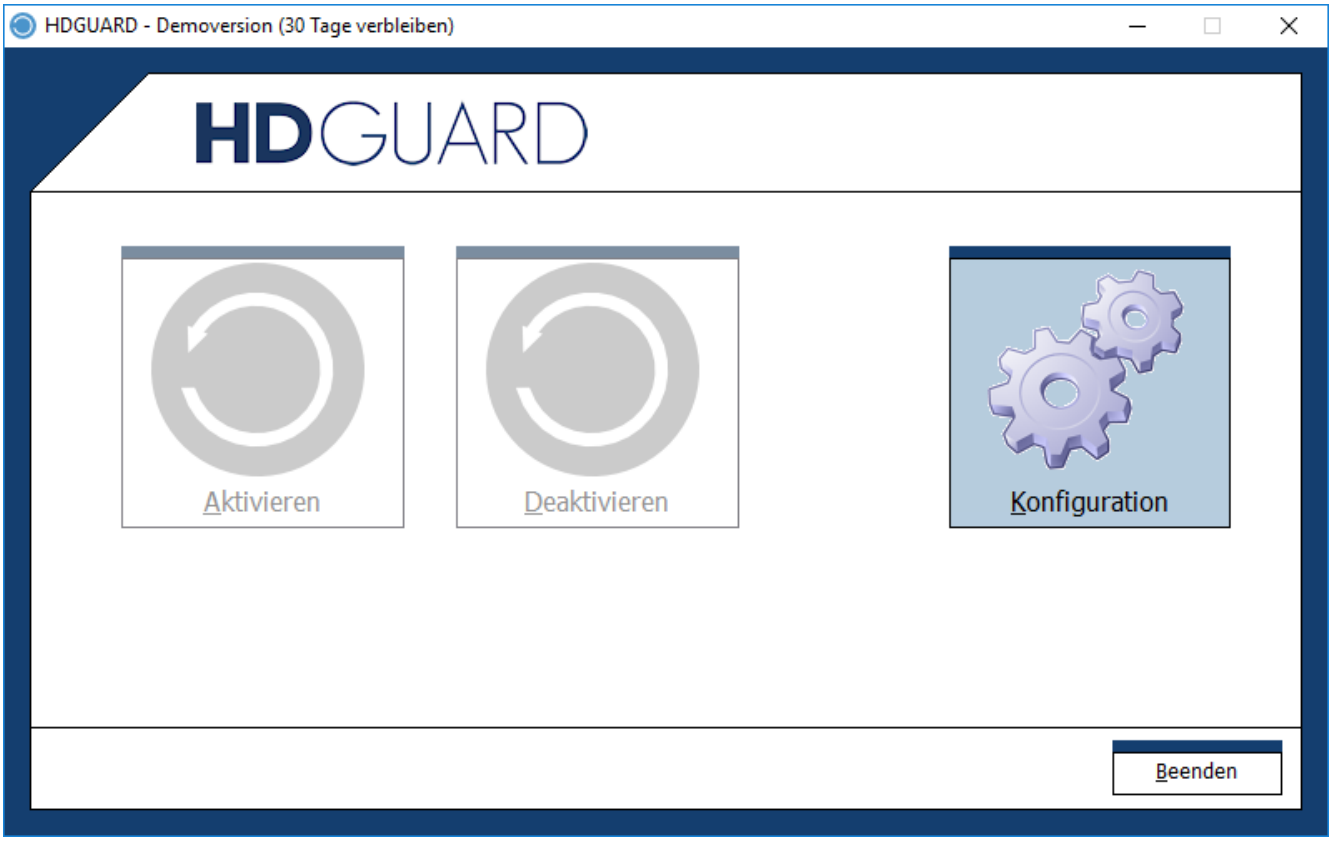
Durch die Aktualisierung der Lizenzinformationen bei der Softwareaktivierung lässt sich beispielsweise eine für mehrere Monate ausgestellte Testlizenz um weitere Monate verlängern bzw. in eine Kauflizenz umwandeln, ohne dass eine neue Lizenz eingegeben werden muss.
Es wird pro HDGUARD geschütztem PC eine Lizenz benötigt. Multibootsysteme benötigen ebenfalls nur eine Lizenz pro PC.

# 4 Die grafische Benutzeroberfläche

Nach der Installation finden Sie HDGUARD auf dem Desktop, im Startmenü, im Traybereich und in seinem Programmverzeichnis.

## 4.1 Erster Start

Doppelklicken Sie das HDGUARD Symbol, um die zentrale Benutzeroberfläche zu öffnen.
Beim Öffnen ohne eingerichteten HDGUARD Schutz wird gefragt, ob eine automatische Konfiguration durchgeführt werden soll. Diese Automatik setzt den Status der eventuell vorhandenen Start- und Bootpartitionen auf „nur Lesen“ und legt eine SWAP-Datei für den Schutz des Systemlaufwerks C: an.



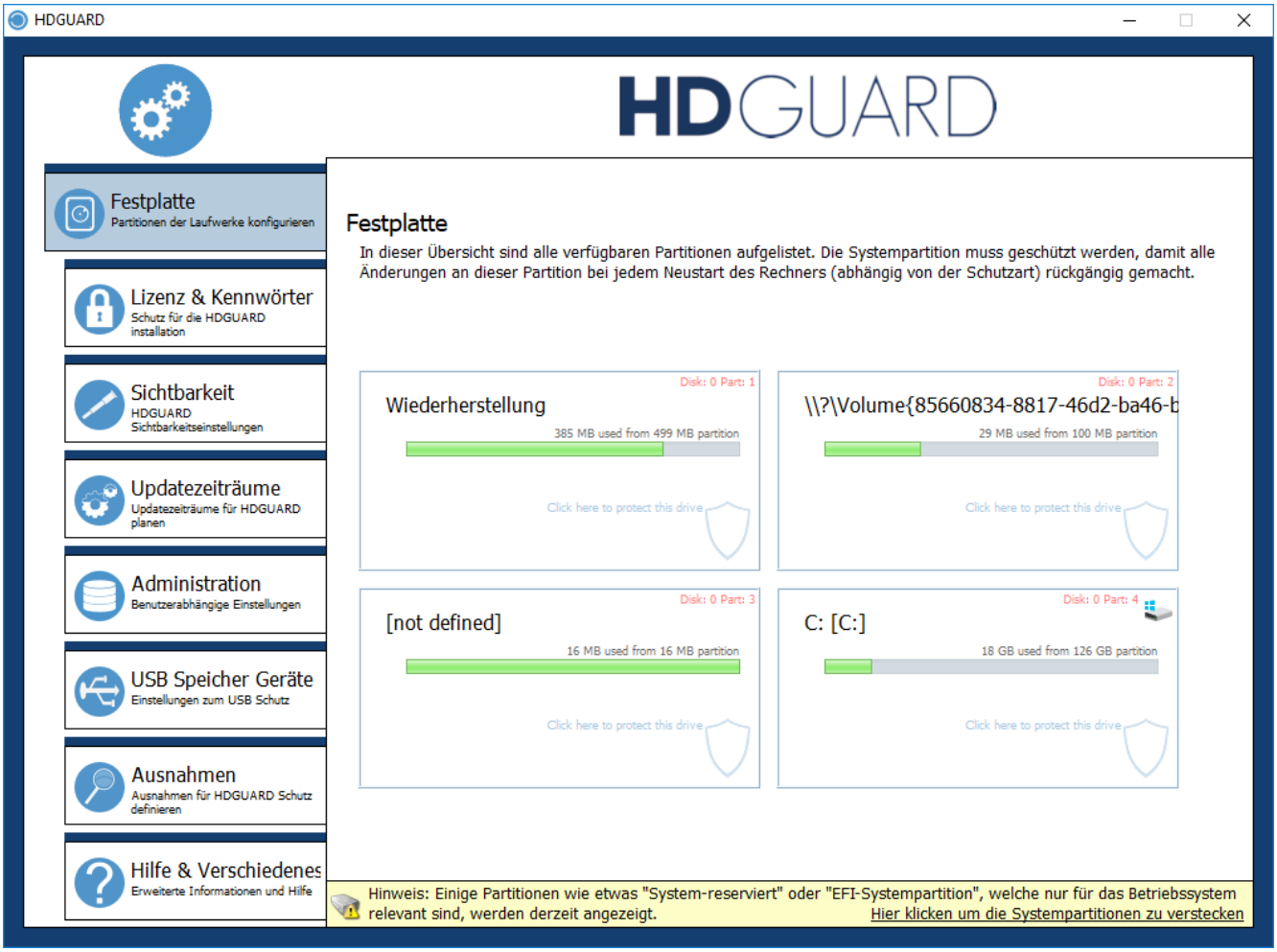

*Der Hauptbildschirm mit deaktivierten Hauptbedienelementen.*

## 4.2 Konfiguration

Drücken Sie den Knopf *Konfiguration,* um ins Konfigurationsmenü zu gelangen.
Die Konfigurationsansicht enthält alles, was Sie für die Anpassung des HDGUARD an Ihre Bedürfnisse benötigen. In den meisten Fällen werden Sie die Konfiguration lediglich einmal vor dem Aktivieren des HDGUARD benötigen. Danach müssen nur selten Änderungen an der Konfiguration vorgenommen werden.

### 4.2.1 Festplatte

Hier bestimmen Sie, welche Partitionen geschützt werden sollen und wo die jeweilige HDGUARD SWAP Datei liegen wird.




*Festplattenkonfigurationsansicht*

Zum Einrichten des Schutzes für Partition *C:* klicken Sie in das Feld von Partition *C:*. Sie werden zunächst nach dem Schutzmodus gefragt. Dieser kann „zu schützen“, „nur lesen“ oder „kein Zugriff“ sein.
Wählen Sie „zu schützen“ aus, so öffnet sich ein Einstellungsfenster, in dem Sie alle verfügbaren Optionen festlegen können. Diese sind:

- Der Ort, wo die SWAP Datei liegen soll. Hinweis: Diese muss auf der gleichen Festplatte liegen.
- Die Größe des Speicherplatzes, der für die SWAP Datei auf der angegebenen Partition reserviert werden soll.
- Die Größe des Hauptspeichers, der reserviert werden soll, um die ersten Umleitungen in die SWAP Datei zu beschleunigen. Nur verfügbar für Systempartitionen.

Für die Option SWAP-RAM wird ein Teil des RAM des PCs belegt, der Start des Betriebssystems jedoch merklich beschleunigt.

### 4.2.2 Lizenz und Kennwörter


*Hier haben Sie die Möglichkeit, Ihre Seriennummer einzugeben und die Softwareaktivierung durchzuführen.*

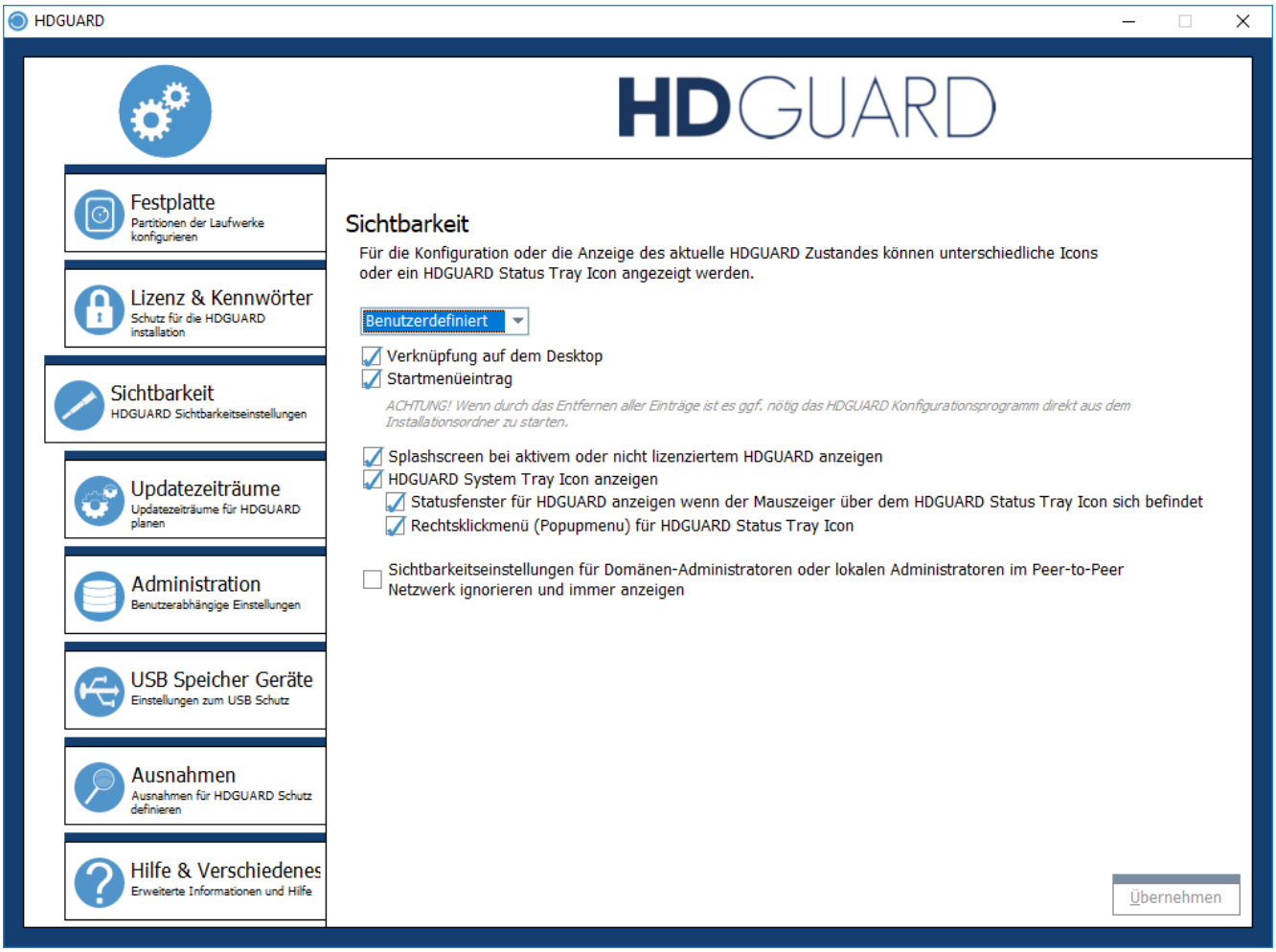
Sollte der aktuelle PC keine Verbindung zum Aktivierungsserver aufbauen können, erhalten Sie die Möglichkeit, die Anfrage in eine Datei zu speichern. Diese Datei kann anschließend auf der Internetseite activation.rdt.de/HDGUARD hochladen und weiterverarbeitet werden. Dieser Schritt kann auch auf einem anderen PC durchgeführt werden.
Im zweiten Tab (auch zu erreichen mit den Knöpfen „Zurück" bzw. „Weiter") wird das HDGUARD Kennwort gesetzt.

Achten Sie unbedingt darauf, Ihr gesetztes Kennwort für den Programmzugriff nicht zu verlegen bzw. zu vergessen. Es gibt keine fest einprogrammierten Kennwörter oder eine Wiederherstellungsmöglichkeit des Kennworts!

Im dritten Tab wird das Kennwort für das Zurücksetzen des Seminarmodus gesetzt. Ohne ein festgelegtes Seminarmoduskennwort kann jeder Benutzer den Seminarmodus zurücksetzen. Siehe Seminarmodus
Im vierten Tab können Sie USB-Geräte definieren, deren Vorhandensein den Passwortschutz des HDGAURD übergeht. Diese Funktion steht zur Verfügung um Lehrern, Servicepersonal oder Aushilfen den Zugang zum Rechner zu gewähren ohne das Kennwort preiszugeben. Ist ein Benutzer über solch einen *Service Key* authentifiziert, so sind Passwortänderungen und das Anlernen weiterer *Service Keys* nicht möglich.

### 4.2.3 Sichtbarkeit

Vielfach liegt es im Interesse des Administrators, dass die Präsenz des HDGUARD vor den Benutzern verborgen bleibt. Der Administrator kann deshalb die Sichtbarkeit des HDGUARD von „voll sichtbar“ bis „unsichtbar“ selbst bestimmen.




Bitte beachten Sie, dass Updateinstallationen (Versionsupdates) vom HDGUARD die Sichtbarkeit teilweise wiederherstellen können.

#### 4.2.3.1 Desktop Icon

Ein HDGUARD Symbol wird auf dem Desktop platziert. Ein Doppelklick auf dieses Symbol startet das HDGUARD Programm.

#### 4.2.3.2 Startmenüeintrag

Einträge für den HDGUARD im Startmenü (unter „Programme\HDGUARD“) anlegen.

#### 4.2.3.3 Splashscreen

Ein Infofenster (engl. Splashscreen) wird bei aktivem HDGUARD angezeigt, so dass der Benutzer über den Schutz des PCs informiert wird.

#### 4.2.3.4 System Tray Icon

Das System Tray (Systray) befindet sich rechts in der Windows Startleiste. Mit Hilfe des angezeigten Symbols, ein Schild in den Farben Blau bis Rot, je nach Auslastung, kann der Zustand des Schutzes angezeigt werden. Es ist ratsam, dieses Symbol immer anzuzeigen.

#### 4.2.3.5 Statusfenster des Tray Icons anzeigen

Beim Bewegen der Maus über das Tray Icon erscheint eine Statusinformation.

### 4.2.4 Updatezeiträume

Um sicherzustellen, dass Ihr Betriebssystem und Ihr Virenscanner immer auf dem aktuellsten Stand sind, können im HDGUARD Updatezeiträume konfiguriert werden.
Während dieser Zeiträume startet der PC ohne den HDGUARD Festplattenschutz und mit restriktiver Benutzeranmeldung. Anmeldungen an den PC werden nicht zugelassen, außer es ist der Benutzer, der im vierten Tab definiert ist. Es können während der Updatezeiträume unbeaufsichtigt Windows Updates eingespielt werden sowie beliebige ausführbare Dateien gestartet werden. Für letztere sowie für eine mögliche automatische Anmeldung mit gesperrtem Bildschirm können im vierten Tab Anmeldeinformationen hinterlegt werden.

In den ersten drei Tabs stellen Sie die Startzeit, Dauer, Anmeldeoptionen und Aktionen der drei unabhängig voneinander definierbaren Updatezeiträume ein.


Sollte die Installation von Windows Updates die Dauer des aktuellen Updatezeitraumes überschreiten, so wird die Dauer automatisch entsprechend verlängert.

Manche Windows Updates benötigen einen Neustart des Systems. Die HDGUARD Steuerung leitet nach dem Einspielen der Updates solche Neustarts ein. Sollten Sie als zugelassener Benutzer während eines solchen Updatezeitraumes eingeloggt sein, wird ein solcher Neustart die Sitzung ohne Nachfrage beenden!

Außer diesen durch den Nutzer konfigurierten Update Zeiträumen gibt es auch spezielle, automatische Update Zeiträume 21.

### 4.2.5 Administration

Mitgliedern der AD Gruppe „HDGUARD-Administrators“ wird die lokale Konfiguration des HDGUARDS erleichtert, indem die Eingabe eines Kennworts beim Start des HDGUARDS entfällt. Die Einrichtung der Gruppe und die Zuordnung der Mitglieder muss zuvor in der Domäne erfolgen.


Auch die AD-Benutzer aus der Gruppe „HDGUARD-Administrators“ müssen lokale Administratorrechte besitzen, sonst ist ein Start der Programmoberfläche nicht möglich.

Weiterhin ist es hier möglich den Namen des PCs anzupassen, auf dem der zentrale Master Dienst installiert wurde.

Der Port darf nicht mit dem Port für die Verbindungen des HDGUARD.master Remote Proxy Dienstes (standardmäßig 25652) verwechselt bzw. in Übereinstimmung gebracht werden!

### 4.2.6 USB Speicher Geräte

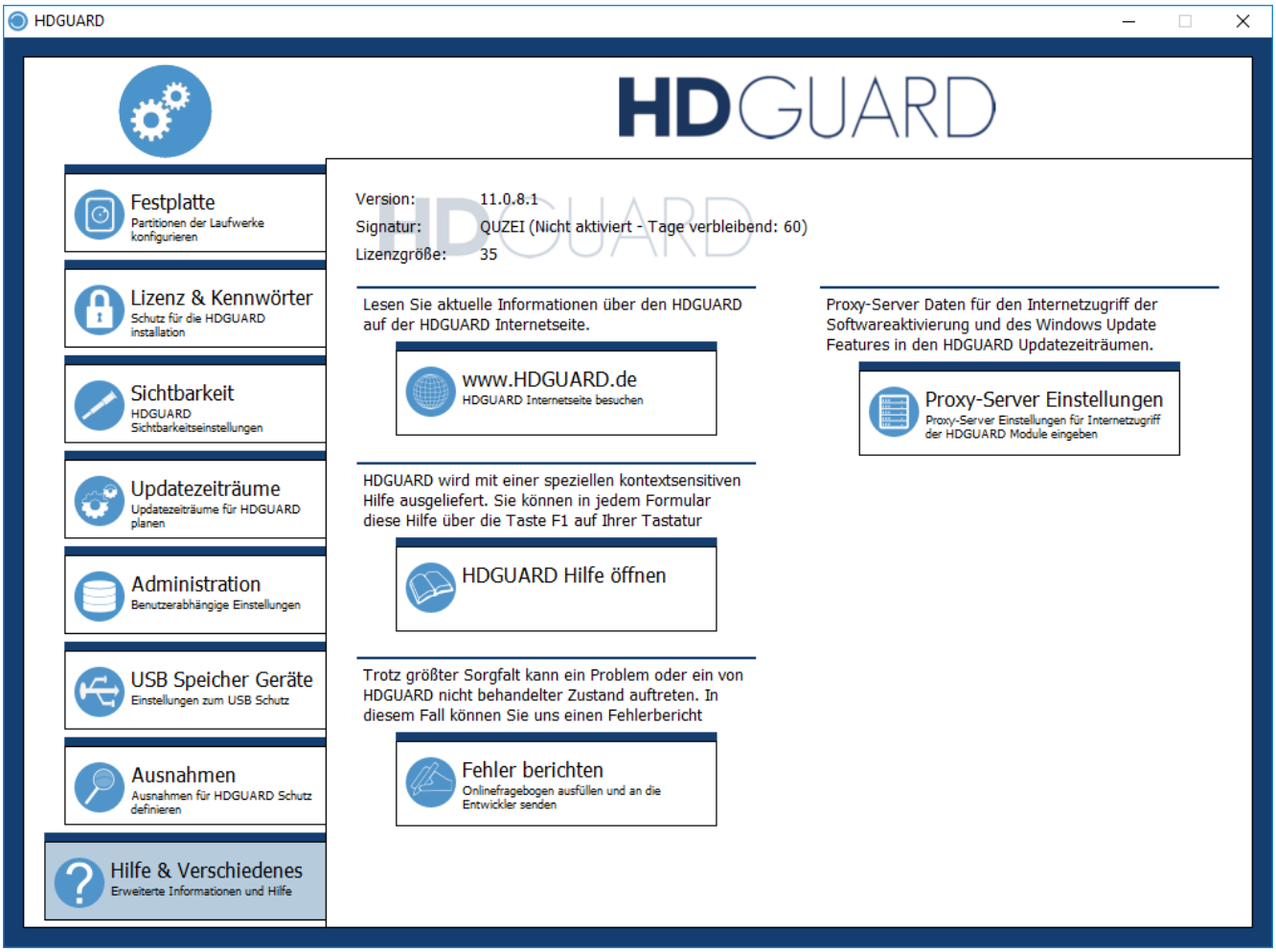
Die HDGUARD Steuerung enthält eine gesonderte Behandlung für USB Geräte der Geräteklasse *USB Massenspeicher* . Diese können entweder mit einem Schreib- bzw. Zugriffsschutz versehen werden.


### 4.2.7 Ausnahmen

Der HDGUARD schützt Ihre Festplatten immer per Partition. Es können also grundsätzlich keine einzelnen Dateien oder Ordner innerhalb einer solchen Partition vom HDGUARD Schutz ausgenommen werden. Gleiches gilt für Einträge in der Systemregistrierungsdatenbank Registry, die ebenfalls in mehreren Dateien auf der Systempartition *C:* abgelegt ist.
Die HDGUARD Konfiguration integriert zwei Techniken, um in engen Grenzen Ordner- und Registryausnahmen realisieren zu können. Dafür wird eine eigene, NTFS formatierte Partition benötigt, welche nicht vom HDGUARD geschützt wird und in der Konfiguration bekannt gegeben werden muss. Ordnerausnahmen werden von der HDGUARD Konfiguration als Ordnerumleitung eingerichtet. Der Ordner liegt augenscheinlich auf der geschützten Partition, jedoch leitet das NTFS Dateisystem den Zugriff auf den angelegten Ordner auf einen versteckten Ordner auf der ungeschützten Partition um.
Registryausnahmen werden durch ein regelmäßiges Backup des angegebenen Registryschlüssels in eine Datei auf der ungeschützten Partition sowie durch ein frühzeitiges Zurückspielen des Backups beim Systemneustart realisiert. Es können somit keine Registryinformationen „ausgenommen“ werden, die für den Betriebssystemstart in irgendeiner Form von Bedeutung sind. Ebenso können keine Schlüssel erfasst werden, die während des Betriebssystemstarts nicht geladen sind, wie zum Beispiel Schlüssel aus dem Zweig des aktuellen Benutzers „HKCU“.

### 4.2.8 Hilfe & Verschiedenes

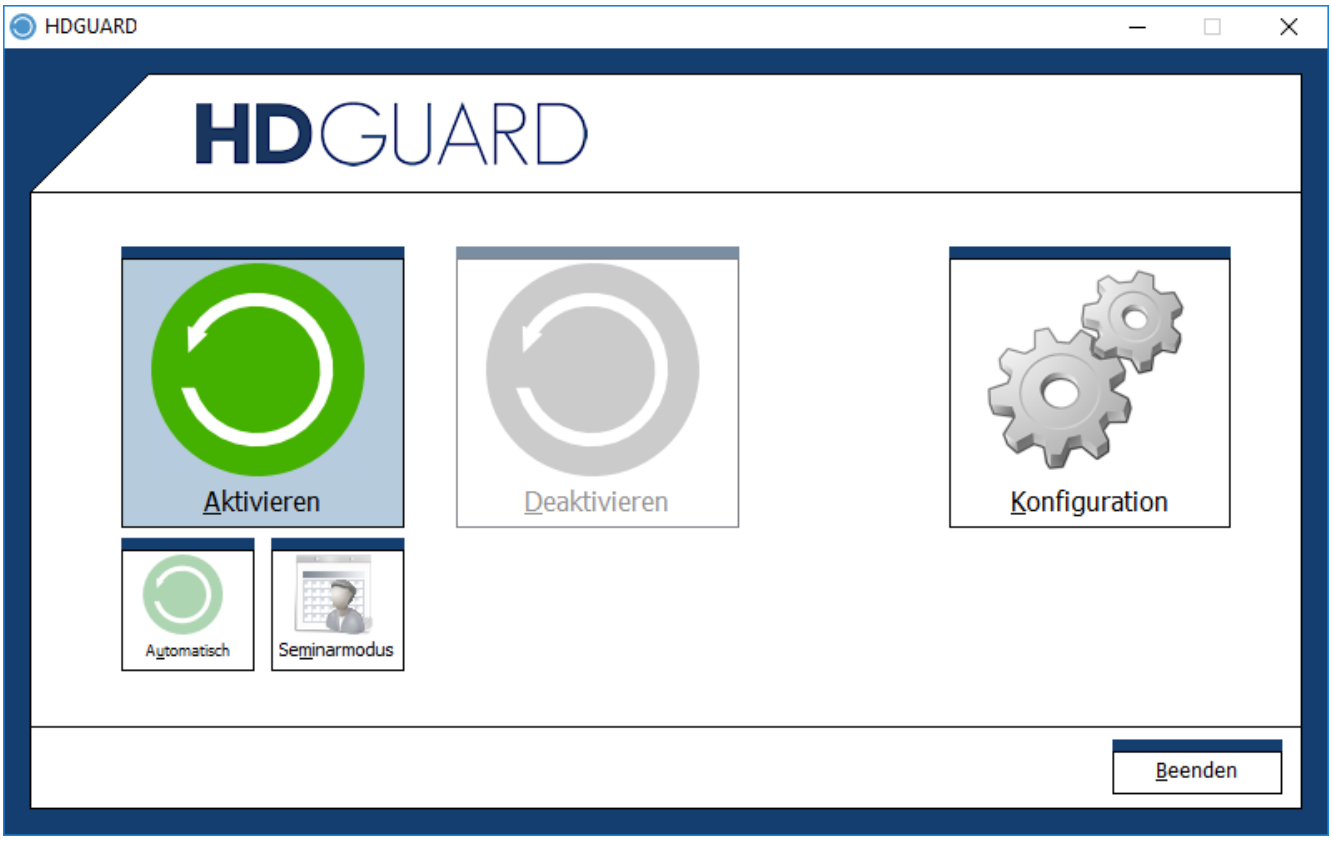
Dieser Konfigurationspunkt zeigt nicht nur Versions- und Lizenzinformationen an, sondern bietet auch die Möglichkeit, die Produktwebseite zu öffnen sowie eine direkte Rückmeldung an die Entwicklung zu geben.




Des Weiteren ist es Ihnen hier möglich eine Proxyverbindung für die Onlineaktivierung und die Updatezeiträume von HDGUARD zu hinterlegen.

## 4.3 Hauptfenster

Nach dem Verlassen der Konfiguration befinden Sie sich wieder im Hauptfenster. Sind die Festplatten eingerichtet, kann der Schutz aktiviert werden.




### 4.3.1 Automatik

Wählen Sie „Aktivieren“ – „Automatisch“, so werden zunächst einige Vorbereitungen für die Zeit des geschützten Systems von der HDGUARD Steuerung vorgenommen. Anschließend wird der Rechner neu gestartet und der Schutz aktiviert. Jeder folgende Neustart setzt den Rechner wieder auf den Zustand zurück, den Sie durch das Drücken auf „Aktivieren“ festgelegt haben.

### 4.3.2 Seminarmodus

Wählen Sie „Aktivieren“ – „Seminarmodus“, weicht die Funktionalität von der automatischen dahingehend ab, dass ein Neustart i.d.R. nicht zum Ursprungszustand des Systems zurückführt. Die Veränderungen aus den vorigen Sitzungen werden solange beibehalten, bis entweder

- der Speicherplatz in der jeweiligen HDGUARD SWAP Datei ausgeschöpft ist oder
- ein Benutzer im Kontextmenü des HDGUARD System Tray Icons die Funktion „Seminarmodus zurücksetzen“ auswählt oder
- ein Updatezeitraum beginnt, dessen Priorität höher als die des Seminarmodus ist.

### 4.3.3 Deaktivieren

Wählen Sie „Deaktivieren“, so endet der HDGUARD Schutz mit einem Neustart des Rechners. Dies setzt den Rechner auf den ursprünglichen Zustand zurück.

# 5 Bedienung per Kommandozeile

Um den HDGUARD auch automatisiert per Skriptsteuerung oder Kommandozeilenterminal zu steuern, starten Sie die ausführbare Datei HDGcmd.exe aus dem Programmverzeichnis mit den entsprechenden Parametern. Ein Aufruf mit unkorrekten oder ohne Parameter zeigt die Kommandozeilenhilfe in Englisch an.

## 5.1 Befehle und Hilfe

```
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!
/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 XXXXXXXXXXXXXXXXXXX
                            :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.
```

## 5.2 Beispiel: 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 Spezielle Updatezeiträume

HDGUARD erkennt die automatische Zeitumstellung aufgrund der Sommerzeitregelung. Der erste Start nach einer Zeitumstellung geschieht ohne HDGUARD Schutz und ohne Möglichkeit einer Benutzeranmeldung. Nach ca. 2 Minuten startet das System automatisch neu mit aktivem HDGUARD Schutz.
Um Bootschleifen durch Windows Updates mit integriertem Neustart zu verhindern, wird ein automatischer Updatezeitraum nach mehreren Neustarts ohne Benutzeranmeldung gestartet. Dieser beendet sich ebenfalls nach ca. 2 Minuten.

# 7 Hilfsfunktionen beim Klonen

Dieser Abschnitt befasst sich mit der Einrichtungshilfe für geklonte HDGUARD Installationen.
Wird eine HDGUARD Installation geklont, so wird i.A. die gesamte Festplattenkonfiguration zurückgesetzt. Daher wird empfohlen, den HDGUARD ohne eingerichtete Festplatten zu klonen. Der erste Start nach dem Klonen wird i.d.R. erkannt und es wird eine automatische Festplattenkonfiguration durchgeführt. Diese lässt sich mit den folgenden Registrywerten parametrisieren.
Im zu erstellenden Registryzweig
`HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\RedirVolumes`

legen Sie dazu einfach für jede Partition, die den HDGUARD Schutz erhalten soll, einen DWORD bzw. einen QWORD Wert an. Benennen Sie den Wert mit dem Pfad des Laufwerks (zum Beispiel *D:*). Geben Sie als Wert die Größe für die SWAP Datei in MByte an.
Für das Systemlaufwerk *C:* wird in jedem Fall eine automatische Konfiguration vorgenommen. Es braucht also nur berücksichtigt zu werden, wenn die SWAP Datei eine von der Automatik abweichende Größe erhalten soll.
Die bei den neueren Windowsversionen automatisch angelegten Startpartitionen erhalten automatisch die Einrichtung „Nur Lesen".
Ist ein HDGUARD Passwort eingerichtet, so muss dieses im Schlüssel
HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\EncPasswords
mit der Verschlüsselung der „HDGcmd.exe" (siehe voriger Abschnitt) hinterlegt werden. Der Wert wird als einfache Zeichenfolge *REG_SZ* mit den Namen „PWD" abgespeichert.
Ist ein Lizenzschlüssel vor dem Klonen eingegeben worden, so versucht der HDGUARD Dienst abschließend eine Internetverbindung zum Softwareaktivierungsserver von IST aufzubauen und die Softwareaktivierung durchzuführen. Liegt keine direkte Internetverbindung vor so können Sie im Zweig
HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\InternetProxy
die Einstellungen für Ihren Proxyserver hinterlegen:

- „REG_SZ" Wert „ProxyNameOrIP" für die Adresse oder den Namen des Servers.
- „REG_DWORD" Wert „Port" für den Port des Zugangs.
- Ggf. „REG_SZ" Wert „LoginName" für den Anmeldenamen für die Verbindung.
- Ggf. „REG_SZ" Wert „Password" für das zugehörige Passwort.

Nach der automatischen Konfiguration wird der Zweig
HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig
automatisch gelöscht.

# 8 HDGUARD.master - Verbindung

Um einzelne HDGUARD Clients mit dem optionalen Programm HDGUARD.master administrieren zu können, muss eine TCP/IP-Verbindung zum entsprechenden PC oder Server mit installiertem zentralen HDGUARD.master Dienst aufgebaut werden. Diese Verbindung wird vom HDGUARD Client aufgebaut.
Während der Installation des HDGUARDs wird der (DNS-)Name bzw. die IP und ggf. ein abweichender Port der Verbindung abgefragt und in der Registry gespeichert. Ohne explizite Einstellung werden folgende Werte benutzt:

- Name: HDGUARDmaster
- Port: 52234

Der Port darf nicht mit dem Port für die Verbindungen des HDGUARD.master Remote Proxy Dienstes verwechselt bzw. in Übereinstimmung gebracht werden!

In größeren Netzwerken empfiehlt es sich, einen Alias (CNAME) im DNS-Server für den Server, auf welchem der zentrale HDGUARD.master Dienst installiert ist, einzutragen.
Sollte dies nicht möglich sein oder muss ein abweichender Port auf dem Rechner mit dem zentralen HDGUARD.master Dienst genommen werden, so können dem HDGUARD Setup auch per Kommandozeile die Einstellungen übergeben werden. Bei einer unbeaufsichtigten Installation sähe die Kommandozeile wie folgt aus:
msiexec /i HDGUARD11_64.msi /qn HDGMASTERNAME=MyHDGUARDmasterPC HDGMASTERPORT=50000 INSTALL_TEACHER=yes
Eine nachträgliche Änderung der Einstellung geschieht über einen Eingriff in die Registry. Der REG_SZ Wert „Server" und der REG_DWORD Wert „ServerPort" sind im folgenden Schlüssel abgelegt:
HKEY_LOCAL_MACHINE\SOFTWARE\IST\HDGUARD

Die neuen Werte werden beim nächsten Neustart des Systems eingelesen. Vergessen Sie nicht, vor diesem Eingriff den HDGUARD Schutz zu deaktivieren!
Die Lehrerkonsole wird ggf. über den Schalter `INSTALL_TEACHER=yes` mitinstalliert.

# 9 Lehrerkonsole

Die HDGUARD Lehrerkonsole stellt bestimmte Funktionalitäten des HDGUARD.master auf einem Dozentenplatz innerhalb eines HDGUARD.master Raumes zur Verfügung. Sie können HDGUARD Clients aufwecken und herunterfahren sowie den Bildschirm, die Tonausgabe, das Internet oder die Drucker sperren und freigeben.
Dazu lesen Sie bitte den entsprechenden Abschnitt im Handbuch des HDGUARD.master.