

HDGUARD 12

Referenzhandbuch

© 2026 IST Deutschland GmbH



HDGUARD 12 Referenzhandbuch

© 2026 IST Deutschland GmbH

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der IST Deutschland GmbH dar. Die Software, die in diesem Dokument beschrieben ist, wird unter einer Lizenzvereinbarung zur Verfügung gestellt und darf nur nach Maßgabe der Bedingungen der Vereinbarung benutzt werden. Es ist rechtswidrig, die Software auf ein anderes Medium zu kopieren, soweit das nicht ausdrücklich in der Lizenzvereinbarung erlaubt ist.

Ohne schriftliche Erlaubnis der IST Deutschland GmbH darf weder dieses Handbuch noch Teile davon für irgendwelche Zwecke in irgendeiner Form mit irgendwelchen Mitteln, elektronisch oder mechanisch, mittels Fotokopie, durch Aufzeichnung oder mit Informationsspeicherungs- und Informationswiedergewinnungssystemen reproduziert oder übertragen werden.

Alle in diesem Handbuch genannten Firmen- und Produktnamen sind eingetragene Warenzeichen der entsprechenden Hersteller.

Herausgeber:

IST Deutschland GmbH
Bergstraße 23
23843 Neritz
Tel: +49 4531 8804-40
Fax: +49 4531 8804-44
Email: info.de@ist.com
Web: ist.com/de/

IST Deutschland GmbH
HRB 1408, OD Lübeck
Geschäftsführer: Patrick Duda
© 2026 IST Deutschland GmbH



1.	Einführung	5
1.1	HDGUARD	5
1.2	HDGUARD.master	5
2.	Installation	5
2.1	Systemvoraussetzungen	6
2.1.1	Hardware	6
2.1.2	Betriebssysteme	6
2.1.3	Festplatteneinrichtung	6
2.1.4	Freier Speicher	6
2.2	Art des HDGUARD Schutzes und Einschränkungen	6
2.3	Installation über die Benutzeroberfläche	7
2.4	Installation in einen Klon-Master	9
2.5	Installation und Einrichtung eines Multibootsystems	10
3.	Lizenzierung und Testzeitraum	11
3.1	Testzeitraum	11
3.2	Lizenzierung	11
3.3	Softwareaktivierung	11
4.	Die grafische Benutzeroberfläche	12
4.1	Erster Start	12
4.2	Konfiguration	12
4.2.1	Festplatte	13
4.2.2	Lizenz und Kennwörter	14
4.2.3	Sichtbarkeit/Seminar	15
4.2.3.1	Desktop Icon	16
4.2.3.2	Startmenüeintrag	16
4.2.3.3	Splashscreen	16
4.2.3.4	System Tray Icon	16
4.2.3.5	Statusfenster des Tray Icons anzeigen	16
4.2.3.6	Seminarmodus-Rücksetzeinstellungen	16
4.2.3.7	Benachrichtigungen	18
4.2.4	Updatezeiträume	20
4.2.5	Windows Update	22
4.2.6	Administration	23
4.2.6.1	HDGUARD-Administrators	23
4.2.6.2	HDGUARD.master Einstellungen	24
4.2.6.3	HDGUARD.remote Internetgateway verwenden	24
4.2.7	USB Speicher Geräte	25
4.2.7.1	Schreibschutz und Schreib- /Leseschutz	26
4.2.7.2	Ausnahmen vom USB Schutz	27
4.2.7.3	Ausnahmen vom USB Schutz Import/Export	29

4.2.8	Ausnahmen	31
4.2.9	Hilfe & Verschiedenes	35
4.3	Hauptfenster	36
4.3.1	Automatik	37
4.3.2	Seminarmodus	38
4.3.3	Deaktivieren	39
5.	Bedienung per Kommandozeile	40
5.1	Befehle und Hilfe	40
5.2	Beispiel: ListPartitions	42
6.	Spezielle Updatezeiträume	43
7.	Hilfsfunktionen beim Klonen	43
8.	HDGUARD.master - Verbindung	44
9.	MSI -Parameter	45
10.	Lehrerkonsole	45

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 Systemvoraussetzungen

2.1.1 Hardware

Handelsüblicher PC mit Intel x64 oder AMD64 Prozessorarchitektur, einem TPM-Chip auf dem Motherboard, 8 GB RAM und 250 GB Festplatte, SSD (empfohlen mindestens 500 GB).

Unterstützung der ARM64 Prozessorarchitektur auf Windows 11 Systemen.

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

2.1.2 Betriebssysteme

Microsoft Windows 11 jeweils für die Architektur Intel X64 und AMD64

Windows 11 für ARM für Geräte mit ARM64 Prozessorarchitektur

2.1.3 Festplatteneinrichtung

MBR oder GPT mit primären und sekundären Partitionen.

Von HDGUARD berücksichtigte Volumes müssen mit NTFS oder FAT32 formatiert sein.

Partitionszusammenführungen wie dynamische Datenträger werden nicht unterstützt.

2.1.4 Freier Speicher

Mindestens 20 GB freier, zusammenhängender Speicher auf dem Systemlaufwerk C: , empfohlen mindestens 40 GB freier, zusammenhängender Speicher auf dem Systemlaufwerk C:

2.2 Art des HDGUARD Schutzes und Einschränkungen

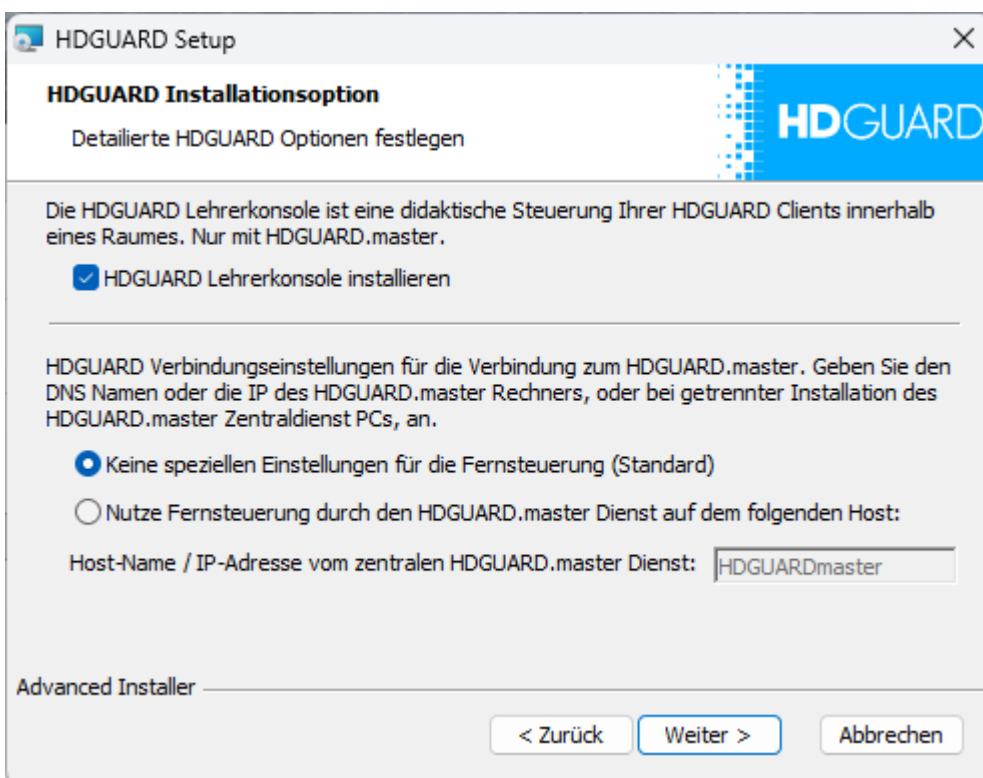
HDGUARD schützt die Daten auf der Festplatte grundsätzlich per Partition. Das heißt, dass alle Änderungen an Registryeinträgen und an Dateien auf dem Systemlaufwerk C: auf jeden Fall durch einen Neustart zurückgesetzt werden. HDGUARD bietet für bestimmte Szenarien Hilfsfunktionen an, mit denen sich diese Einschränkungen abmildern lassen. Es wird empfohlen, [Updatezeiträume](#)^[20] zu nutzen, um bei zeitweise deaktiviertem HDGUARD Schutz Updates etc. einspielen zu können. In seltenen Fällen können auch [Ausnahmen](#)^[31] 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 Schutz aktiv ist.

2.3 Installation über die Benutzeroberfläche

Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen. Starten Sie die Installation durch Aufruf der HDGUARD12_64.msi. Sie erhalten die aktuellen Installationsquellen im Internet unter www.ist.com/de/downloads. Das benötigte Passwort finden Sie in Ihrer Lizenzmitteilung.

Falls die Lehrerkonsole mit installiert werden soll, muss der entsprechende Haken im Setup gesetzt werden. Die nachträgliche Installation ist nicht möglich.



Soll der HDGUARD.master zur Verwaltung der Clients eingesetzt werden, muss im Setup des Clients die Verbindungseinstellung zwischen Client und zentralem Master Dienst hinterlegt werden. Wenn keine speziellen Einstellungen eingetragen werden, wird als Standard der Name HDGUARDmaster genutzt. Dies ist sinnvoll, wenn der Name des PCs, auf dem der zentrale Dienst des Masters eingerichtet ist, HDGUARDMASTER heißt, oder ein entsprechender Alias im DNS eingetragen ist. Auch für Umgebungen ohne den HDGUARD.master ist dies die richtige Einstellung.

In allen anderen Fällen muss die zweite Option gewählt und der DNS Name oder die IP Adresse des PCs eingetragen werden, auf dem der zentrale Dienst eingerichtet wurde.

HDGUARD Setup

HDGUARD Installationsoption
Detaillierte HDGUARD Optionen festlegen

Die HDGUARD Lehrerkonsole ist eine didaktische Steuerung Ihrer HDGUARD Clients innerhalb eines Raumes. Nur mit HDGUARD.master.

HDGUARD Lehrerkonsole installieren

HDGUARD Verbindungseinstellungen für die Verbindung zum HDGUARD.master. Geben Sie den DNS Namen oder die IP des HDGUARD.master Rechners, oder bei getrennter Installation des HDGUARD.master Zentralsdienst PCs, an.

Keine speziellen Einstellungen für die Fernsteuerung (Standard)

Nutze Fernsteuerung durch den HDGUARD.master Dienst auf dem folgenden Host:

Host-Name / IP-Adresse vom zentralen HDGUARD.master Dienst:

Advanced Installer

< Zurück Weiter > Abbrechen

Die [Lehrerkonsole](#)⁴⁵⁾ 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 Ihrem Windows PC HDGUARD12_64.msi. Sie erhalten die aktuellen Installationsquellen im Internet unter www.ist.com/de/downloads. Das benötigte Passwort finden Sie in Ihrer Lizenzmitteilung.

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](#)^[43].

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](#)^[40] 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](#)^[11].

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](#)^[14] und die Anpassung der [Sichtbarkeit](#)^[15] alle Funktionen zur Verfügung.

3.2 Lizenzierung

Nach der Eingabe einer gültigen [Seriennummer](#)^[14] 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 license-de.ist.com 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.

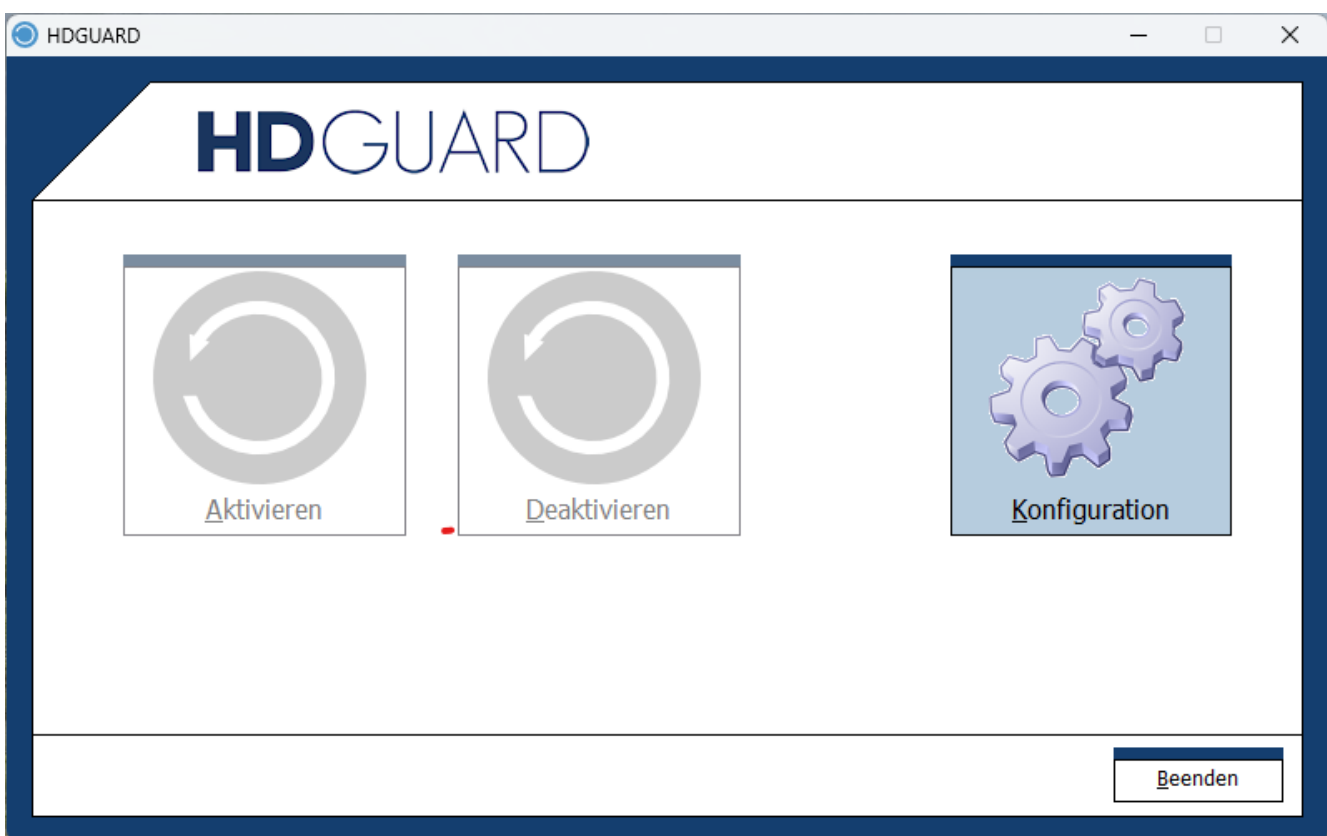
Es wird pro HDGUARD geschütztem PC eine Lizenz benötigt. Multibootsysteme benötigen ebenfalls nur eine Lizenz pro PC.

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 Bedienelementen

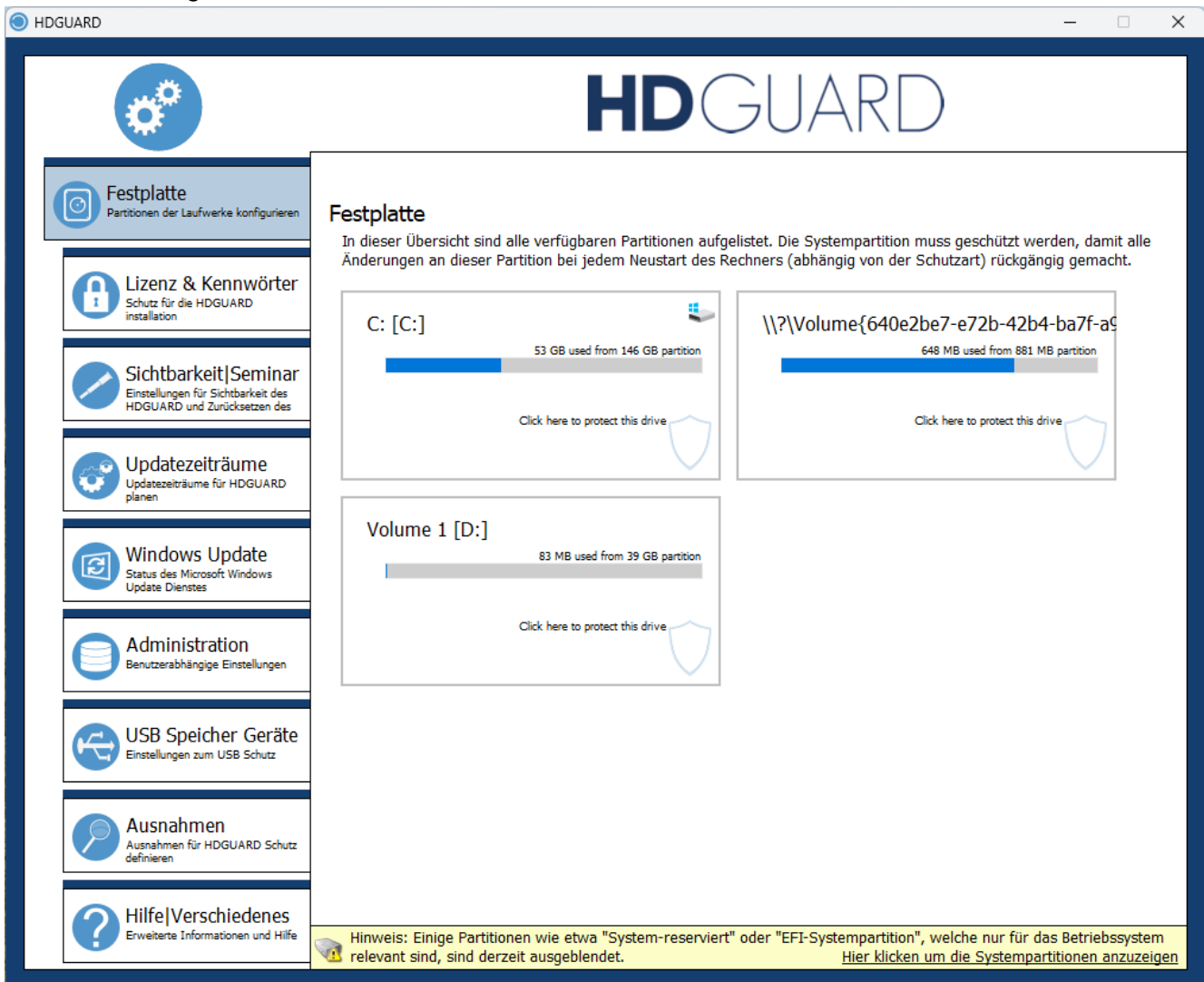
4.2 Konfiguration

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

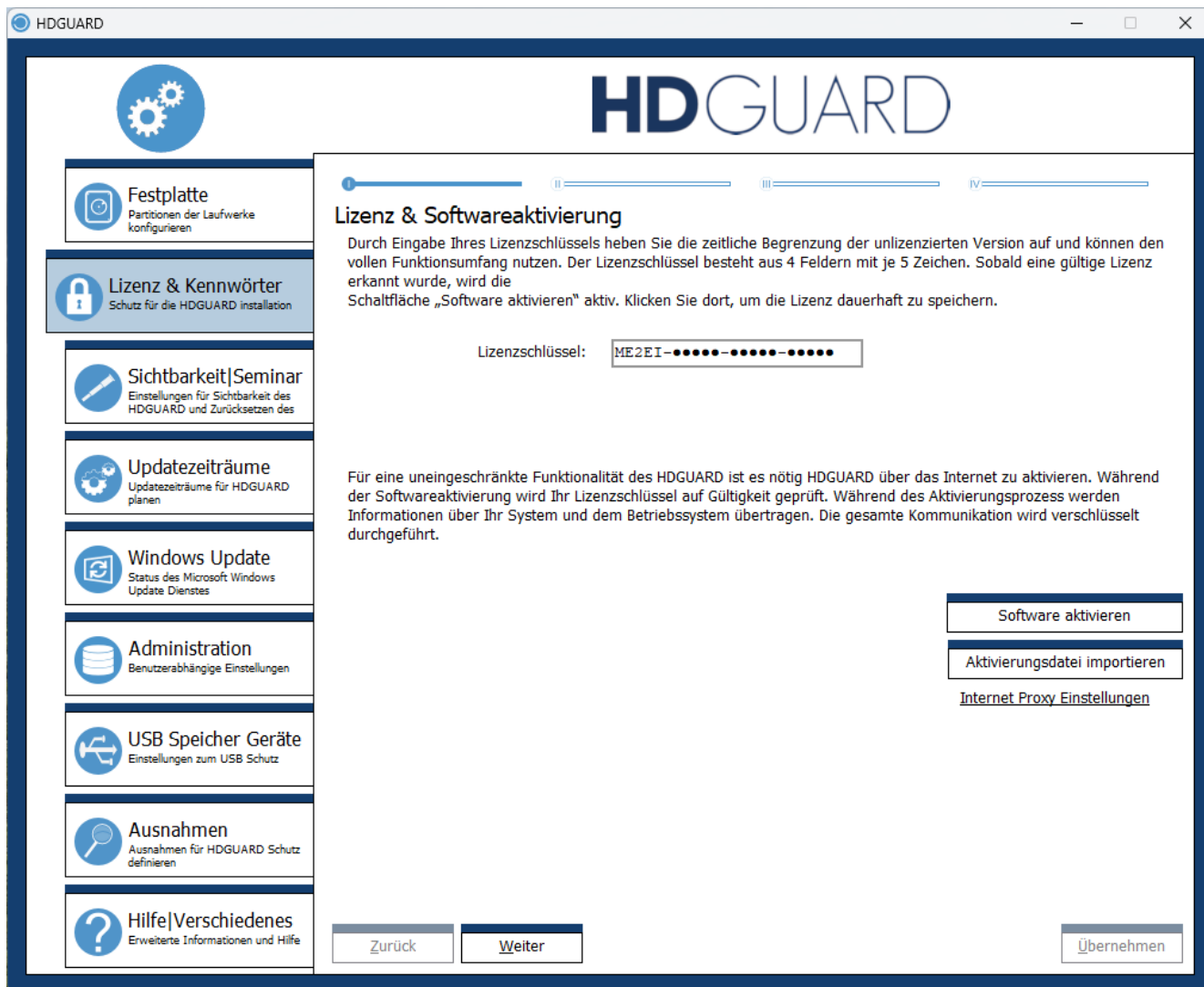
Zum Einrichten des Schutzes für Partition **C:** klicken Sie in das Feld von Partition **C:**. Sie werden zunächst nach dem Schutzmodus gefragt. Dieser kann „zu schützen“, „nur lesen“ oder „kein Zugriff“ sein.

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 auf älteren Festplatte (vor allem HDDs) 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 <https://license-de.ist.com> 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 Programmschutz 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 Seminarmoduskenwort 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/Seminar

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.

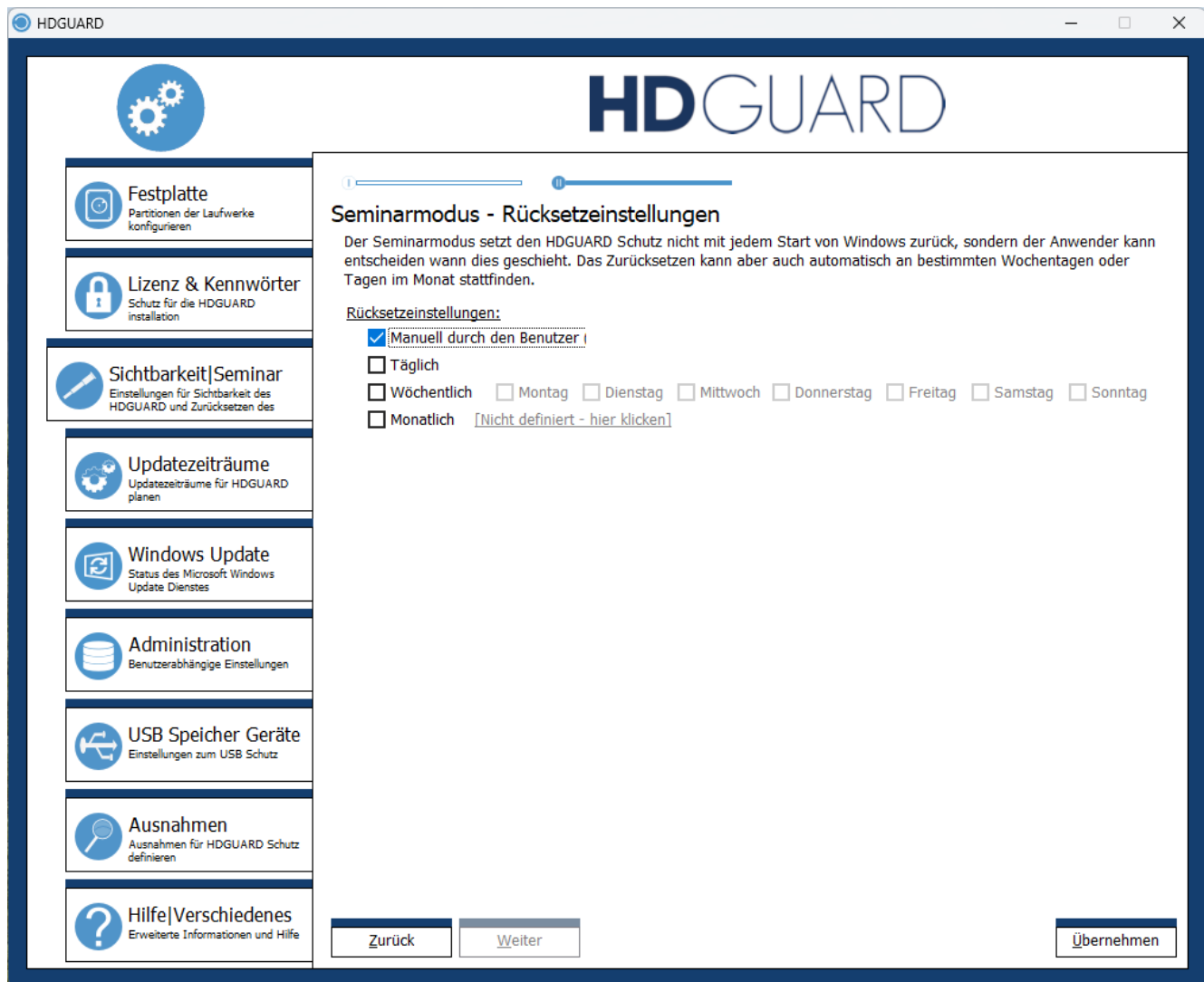
4.2.3.5 Statusfenster des Tray Icons anzeigen

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

4.2.3.6 Seminarmodus-Rücksetzeinstellungen

Im Seminarmodus kann der Anwender entscheiden, wann der Schutz zurückgesetzt werden soll. Das Zurücksetzen des Seminarmodus erfolgt bei der Einstellung **Manuell durch den Benutzer** über das Tray Icon des HDGUARDs und kann mit einem Kennwort geschützt werden. Ohne den Kennwortschutz kann jeder Benutzer das System für den nächsten Neustart zurücksetzen. Das Kennwort kann in [Lizenz und Kennwörter](#)^[14] hinterlegt werden.

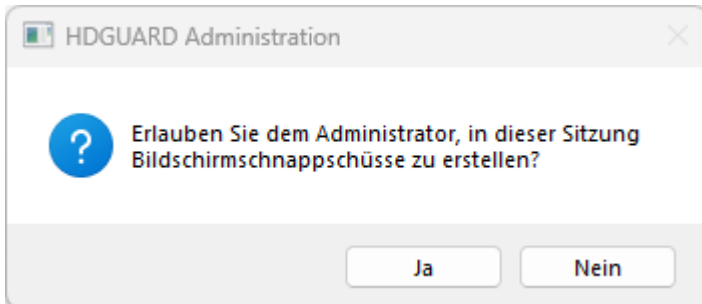
Es ist ebenfalls möglich das Zurücksetzen täglich, an bestimmten Wochentagen oder Tagen im Monat automatisch durchzuführen.



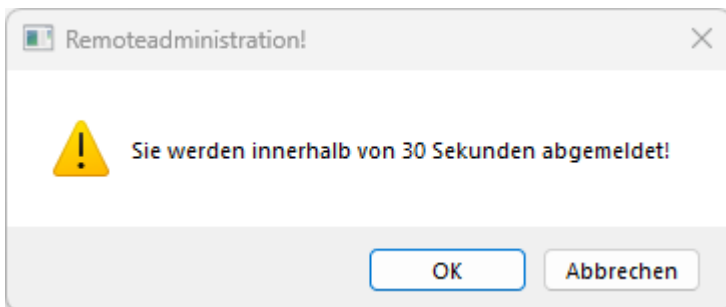
Bevor die Aktivierung des Schutzes im Seminarmodus genutzt werden kann, müssen die Rücksetzeinstellungen definiert werden.

4.2.3.7 Benachrichtigungen

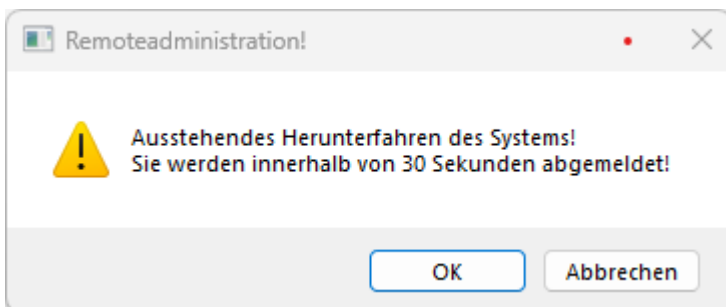
Wenn über den HDGUARD.master ein Screenshot eines Clients angefordert wird, muss dies der Benutzer zulassen. Es wird für die Dauer von 25 Sekunden ein Fenster eingeblendet, das dem angemeldeten Benutzer die Möglichkeit bietet, den Screenshot zuzulassen oder abzulehnen.



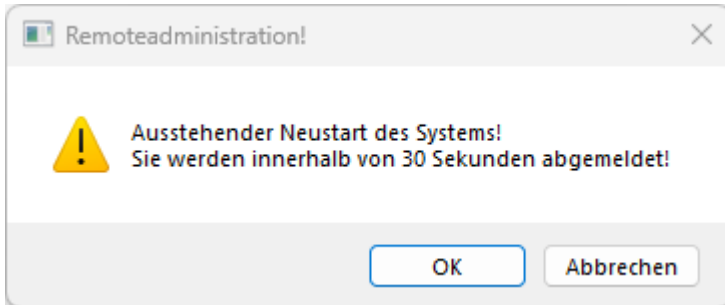
Der HDGUARD.master bietet für Wartungszwecke die Möglichkeit Benutzer remote abzumelden. Falls Benutzer angemeldet sind, können sie die Abmeldung innerhalb von 30 Sekunden abbrechen.



Mit Hilfe des HDGUARD.masters ist es möglich, PCs ferngesteuert herunterzufahren. Hierüber wird der angemeldete Benutzer informiert und kann dies innerhalb von 30 Sekunden abbrechen.



Eine weitere Benachrichtigung wird eingeblendet, wenn der PC vom HDGUARD.master remote neu gestartet werden soll. Auch hier besteht für den angemeldeten Benutzer die Möglichkeit diesen Vorgang abubrechen.



Die Benachrichtigungen werden nur eingeblendet, wenn im HDGUARD.master ausgewählt wurde, dass der angemeldete Benutzer über die geplante Aktion eine Benachrichtigung erhalten soll. In allen anderen Fällen wird die Aktion unverzüglich durchgeführt.

Eine Ausnahme hiervon ist die Erstellung eines Screenshots. Es wird immer eine Benachrichtigung eingeblendet, die dem Benutzer die Möglichkeit bietet den Vorgang abubrechen.

4.2.4 Updatezeiträume

Um sicherzustellen, dass Ihr Betriebssystem und Ihr Virens Scanner 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.



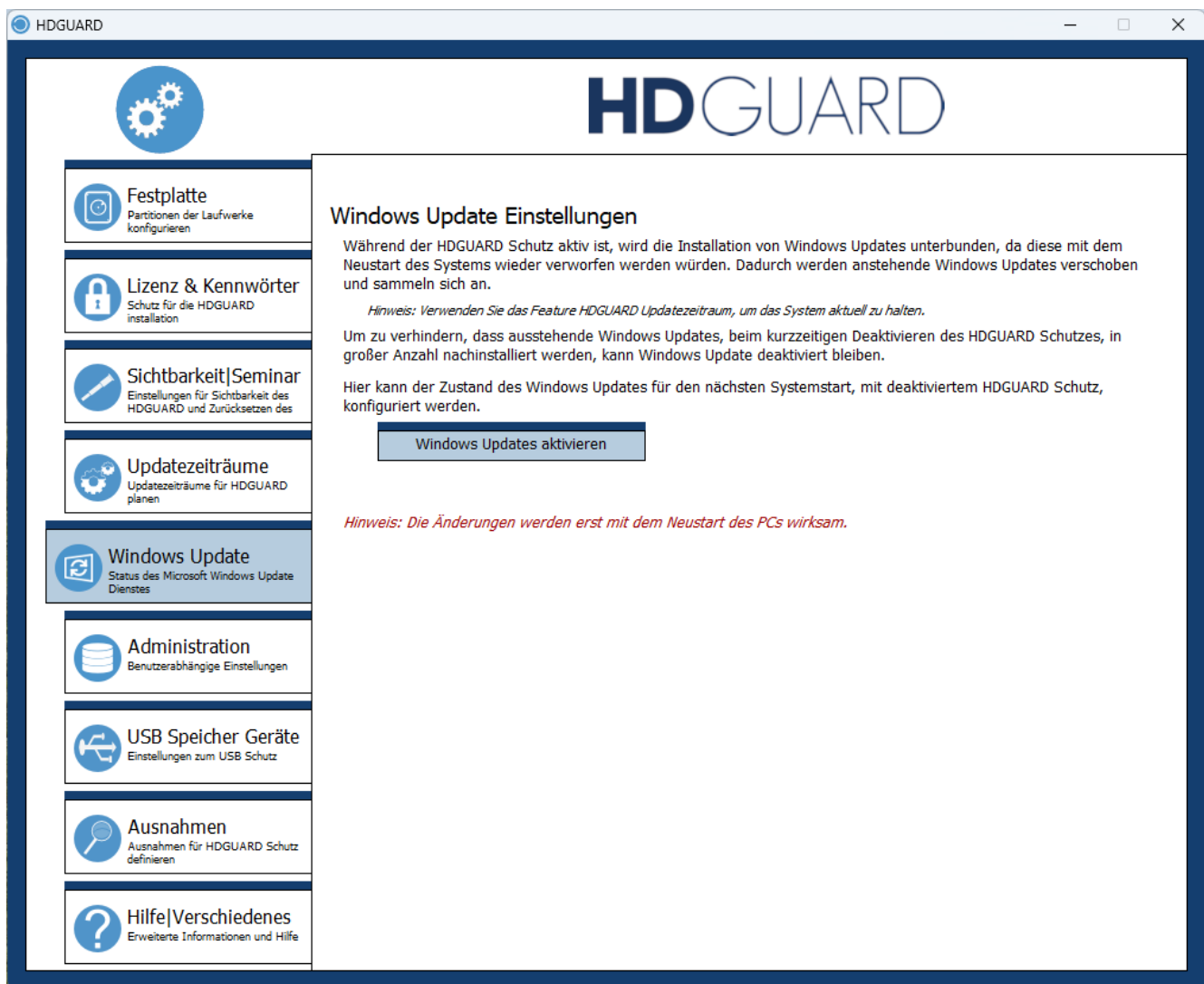
Sollte die Installation von Windows Updates die Dauer des aktuellen Updatezeitraumes überschreiten, so wird die Dauer automatisch entsprechend verlängert.

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](#) ^[43].

4.2.5 Windows Update

Bei aktiviertem Schutz wird die Installation von Windows Updates unterbunden. Mit deaktiviertem Schutz wird die Updatefunktion des Betriebssystems wieder aktiviert. Falls von diesem Standard beim Deaktivieren des Schutzes abgewichen wird und die Updatefunktion auch bei deaktiviertem Schutz weiterhin deaktiviert bleiben soll, kann dies in der Konfiguration des HDGUARDs unter **Windows Update** wieder geändert werden.



Nach der Auswahl von **Windows Updates aktivieren** und dem Neustart des Systems können Windows Updates installiert werden.

4.2.6 Administration

Die Schaltfläche Administration bietet verschiedene Konfigurationsmöglichkeiten für die Einrichtung des Clients. Hier können z.B. die Verbindung zum HDGUARD.master und die Aktivierung von HDGUARD.remote vorgenommen werden.

4.2.6.1 HDGUARD-Administrators

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.

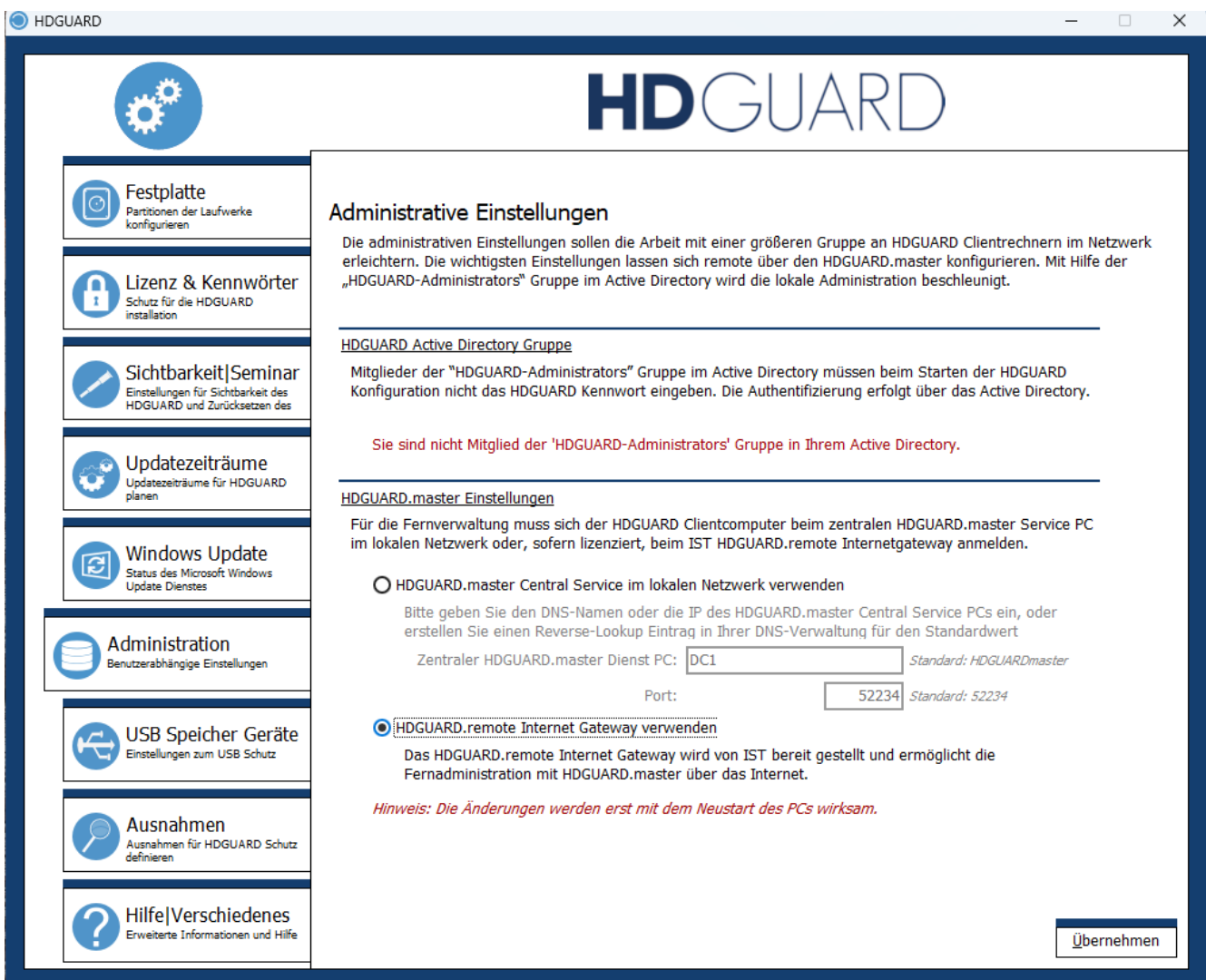
4.2.6.2 HDGUARD.master Einstellungen

In den HDGUARD.master Einstellungen kann die Verbindung der Clients zum HDGUARD.master geändert werden, indem der Name oder die IP Adresse des PCs, auf dem der zentrale Dienst des HDGUARD.masters installiert wurde, angepasst wird. Der Port sollte beibehalten werden. Ist es erforderlich, den Standardport zu ändern, weil Applikationen oder Geräte diesen Port bereits nutzen, nehmen Sie bitte Kontakt zum Support auf.

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

4.2.6.3 HDGUARD.remote Internetgateway verwenden

Falls HDGUARD.remote lizenziert ist, muss das Internetgateway auf den Clients eingerichtet sein. Hierfür muss der Menüpunkt **HDGUARD.remote Internet Gateway verwenden** aktiviert werden.



Eine Internetverbindung zum SSL-gesicherten IST Server hdgremote.ist.com muss über das Internet erreichbar sein.

4.2.7 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.



4.2.7.1 Schreibschutz und Schreib-/Leseschutz

USB Speicher Geräte können mit einem Schreib- bzw. Zugriffsschutz versehen werden.

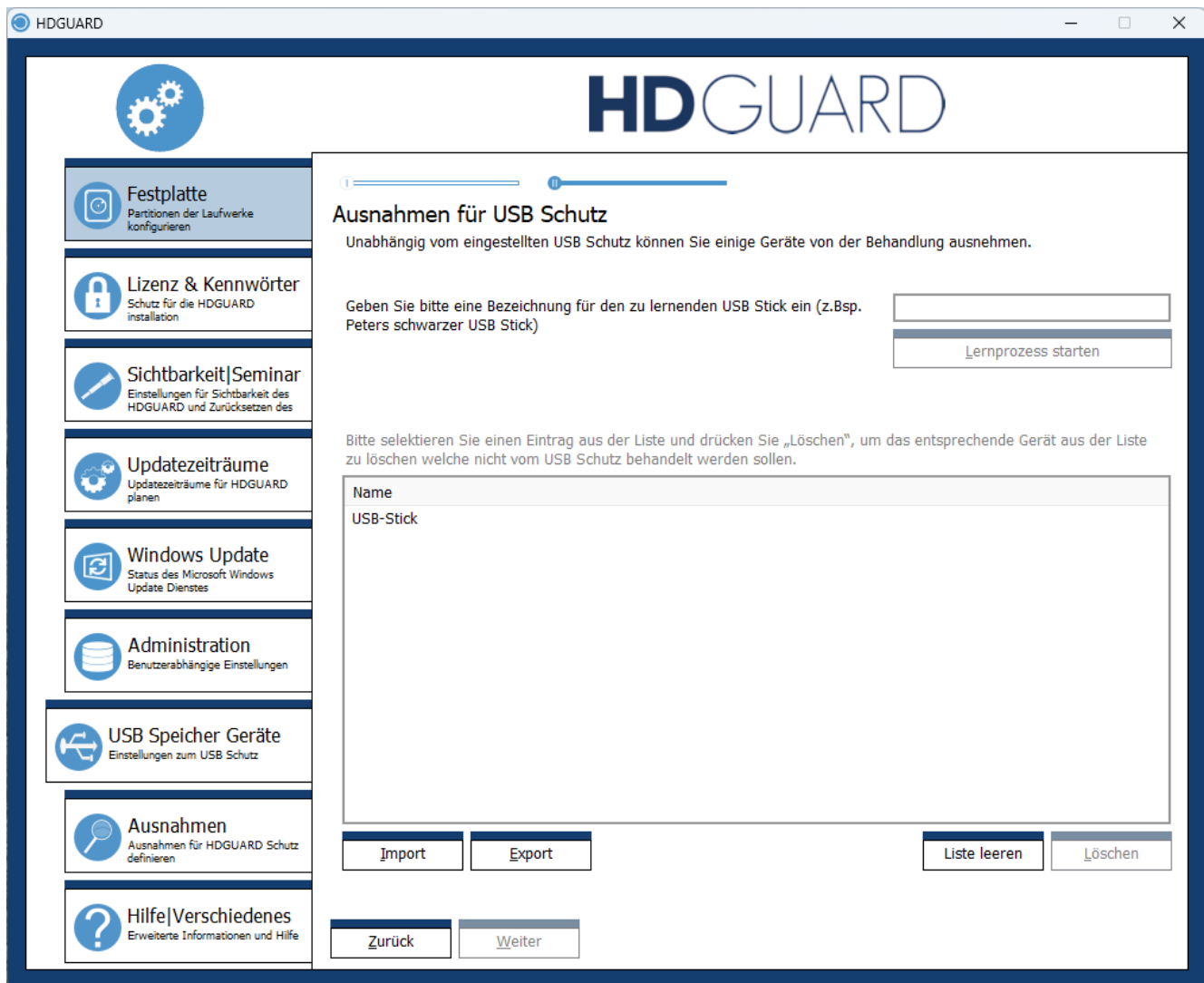


4.2.7.2 Ausnahmen vom USB Schutz

Unabhängig vom eingestellten USB Schutz können einzelne Geräte von der Sperre ausgenommen werden. Der Zugriff auf diese Geräte ist immer möglich. Zunächst muss eine Bezeichnung für das Gerät angegeben werden. Anschließend muss das Gerät angelernt werden.



Der Lernprozess wird durch einen Klick auf **Lernprozess starten** ausgelöst. Innerhalb von 15 Sekunden muss der USB Stick an das Gerät angeschlossen werden. Ist der Vorgang erfolgreich, wird dies in der Oberfläche des Konfigurationsmenüs angezeigt und der Stick kann nun verwendet werden.



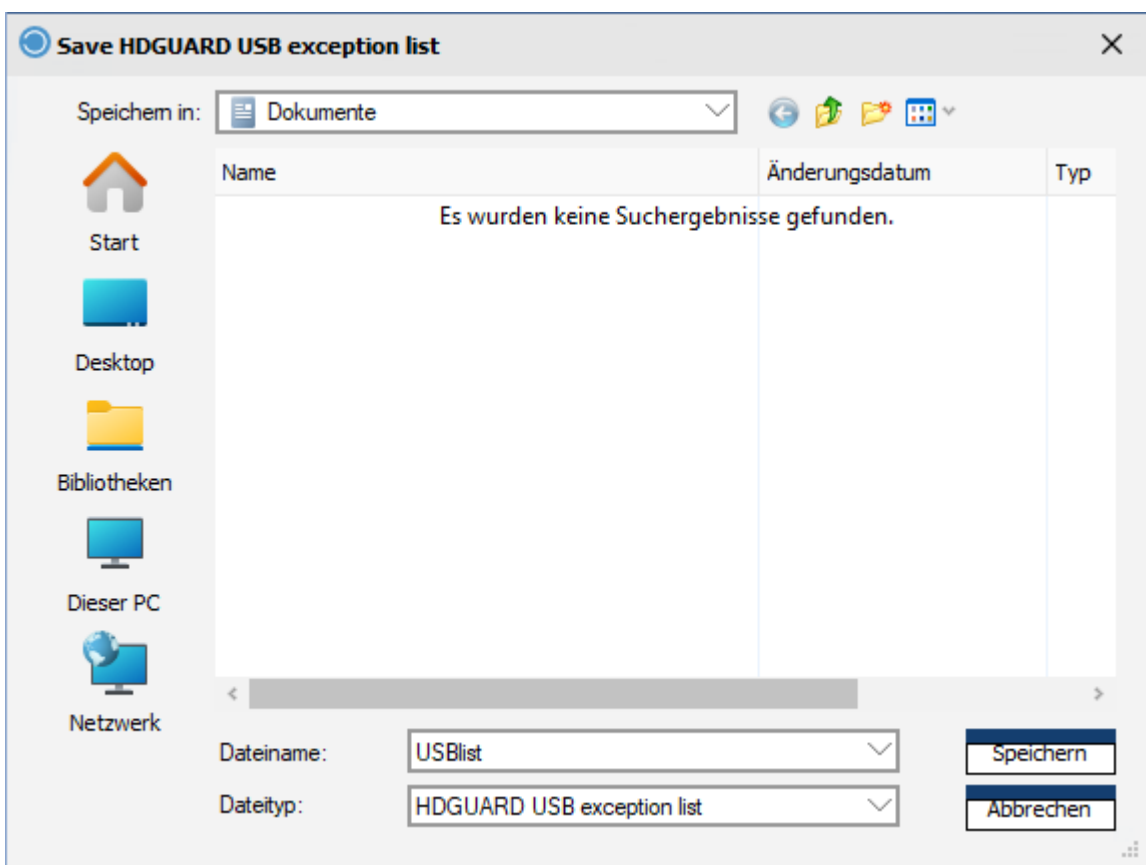
Der Lernprozess muss an allen Geräten durchgeführt werden, an denen der USB Stick von der USB Sperre ausgenommen werden soll.

4.2.7.3 Ausnahmen vom USB Schutz Import/Export

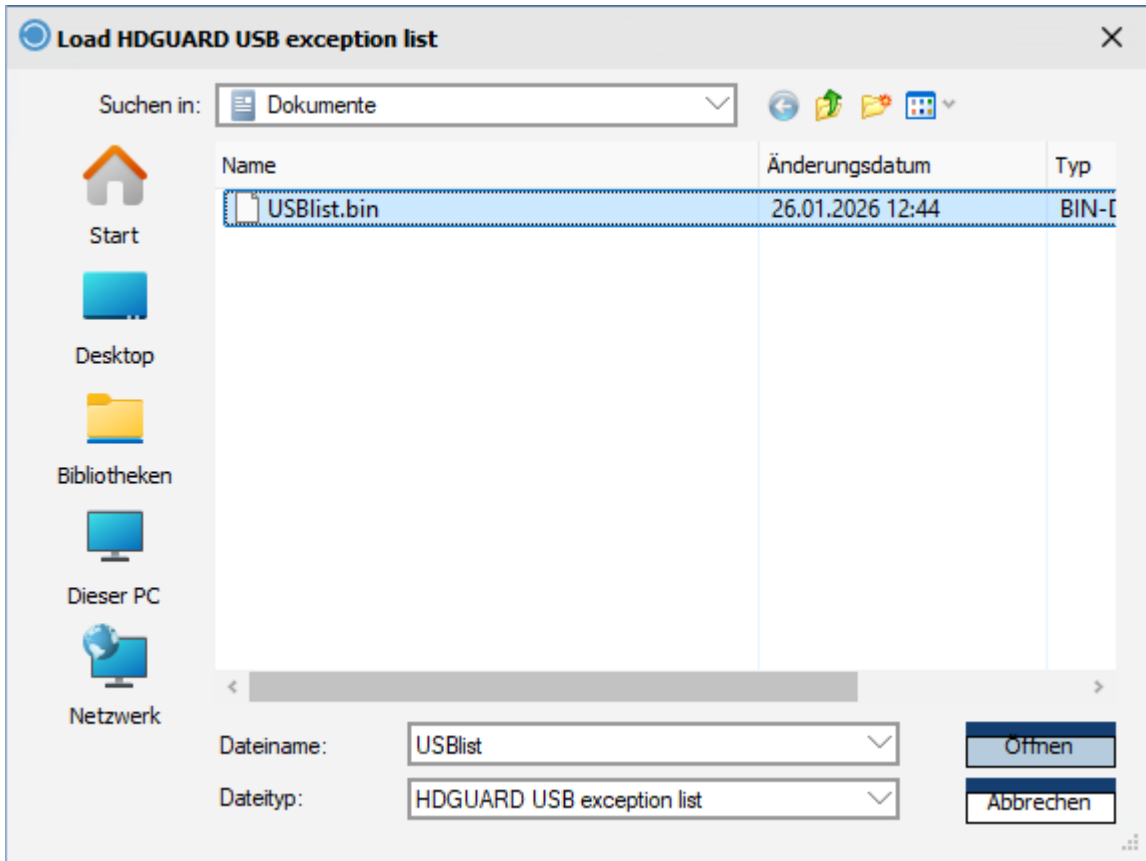
Wenn mehrere USB Sticks von der Behandlung durch die USB Sperre ausgenommen werden sollen, ist es möglich, diese an einem PC anzulernen und die Konfiguration zu exportieren, um sie auf weiteren PCs importieren zu können. Die Exportliste wird für diesen Zweck auf einem externen Datenträger, z.B. einem USB Stick, gespeichert.

Die Im- und Exportfunktion befindet sich auf der Maske, in der auch die Ausnahmen für den USB Schutz definiert wurden.

Der Export wird über die Schaltfläche **Export** gestartet und auf einem beliebigen Laufwerk gespeichert. Im Beispiel ist dies ein USB Stick.



Die Liste der vom USB Schutz ausgenommenen USB Sticks kann nun auf allen PCs mit der Schaltfläche **Import** importiert werden, auf denen USB Sticks genutzt werden sollen, auch wenn die USB Sperre aktiv ist.

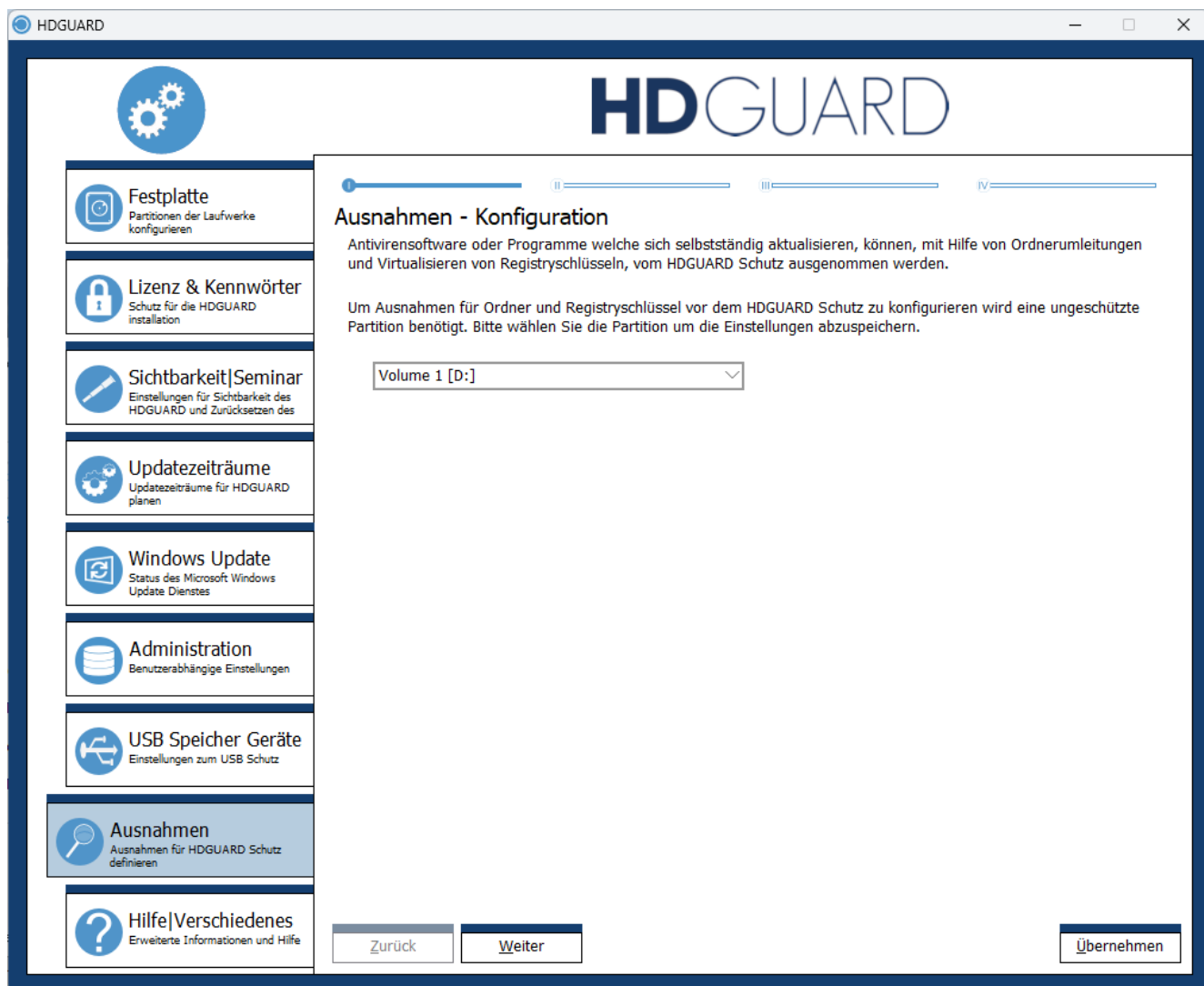


4.2.8 Ausnahmen

HDGUARD schützt Festplatten immer per Partition. Es können 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.

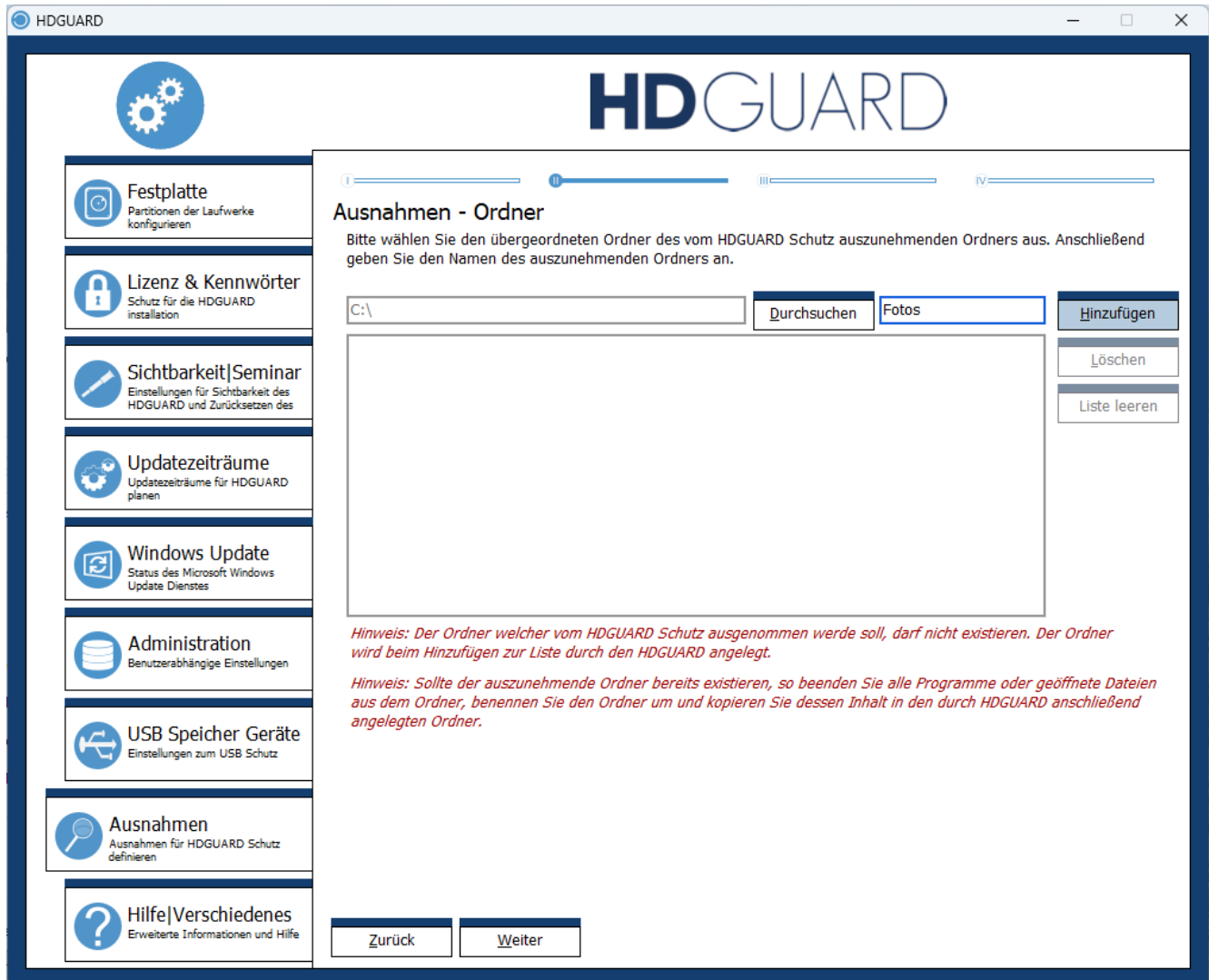
Ordnerausnahmen werden von der HDGUARD Konfiguration als Ordnerumleitung eingerichtet. Der Ordner liegt augenscheinlich auf der geschützten Partition, jedoch leitet das NTFS Dateisystem den Zugriff auf den angelegten Ordner auf einen versteckten Ordner auf der ungeschützten Partition um. Registryausnahmen 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“.

Für die Realisierung von Ausnahmen wird eine eigene, NTFS formatierte Partition benötigt, welche nicht vom HDGUARD geschützt wird und in der Konfiguration bekannt gegeben werden muss.



Die ungeschützte Partition wird ausgewählt und die Auswahl erfolgt mit **Übernehmen** und **Weiter**.

Im nächsten Schritt muss ein übergeordneter Ordner über die Schaltfläche **Durchsuchen** ausgewählt und der Name des Verzeichnisses hinterlegt werden, das umgeleitet werden soll.



Die Einrichtung wird mit **Hinzufügen** abgeschlossen.



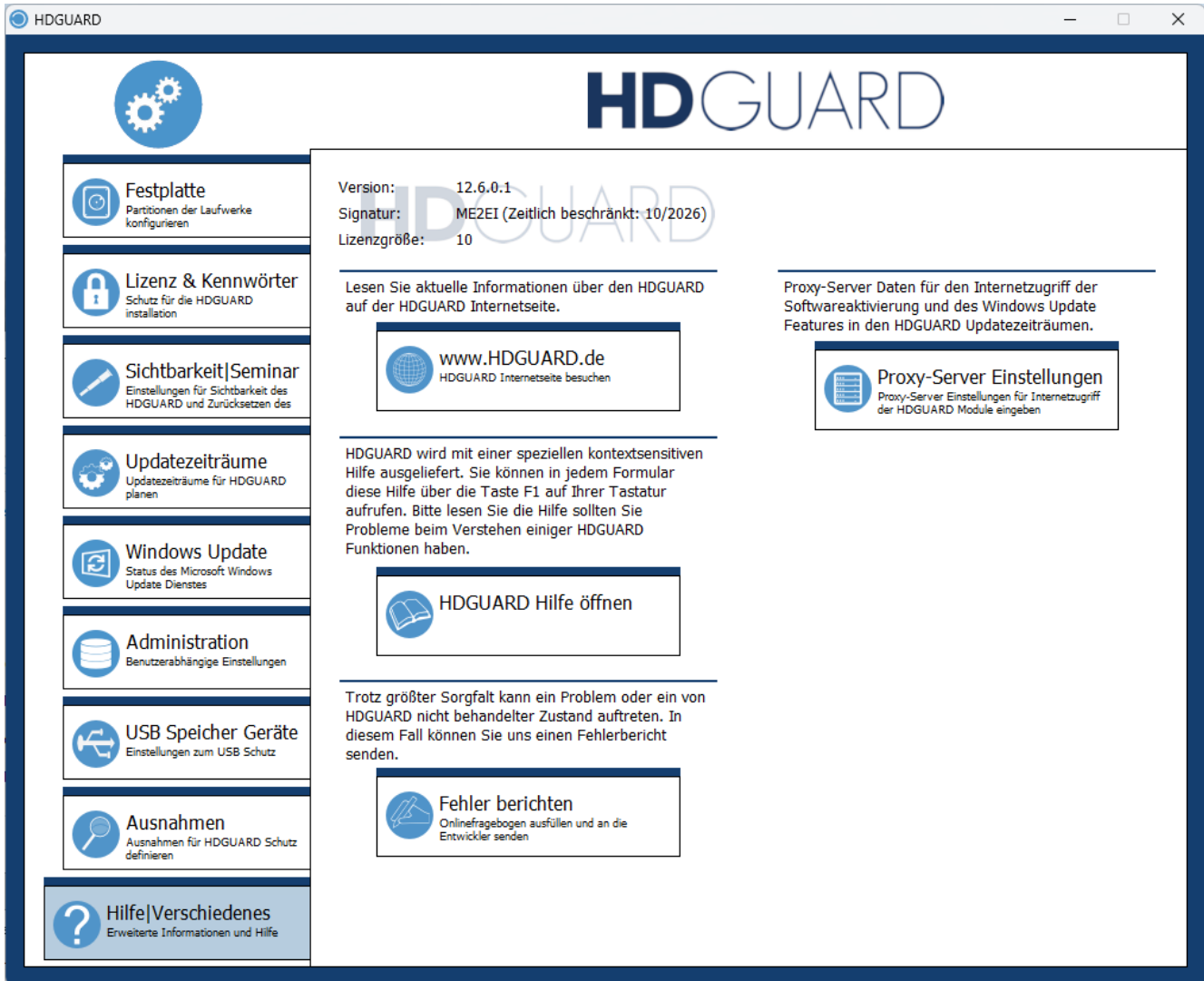
Um Registryschlüssel vom Schutz auszunehmen, werden diese mit **Durchsuchen** ermittelt und anschließend hinzugefügt.



Die Konfiguration wird sofort übernommen und muss nicht mit OK oder Weiter bestätigt werden.

4.2.9 Hilfe & Verschiedenes

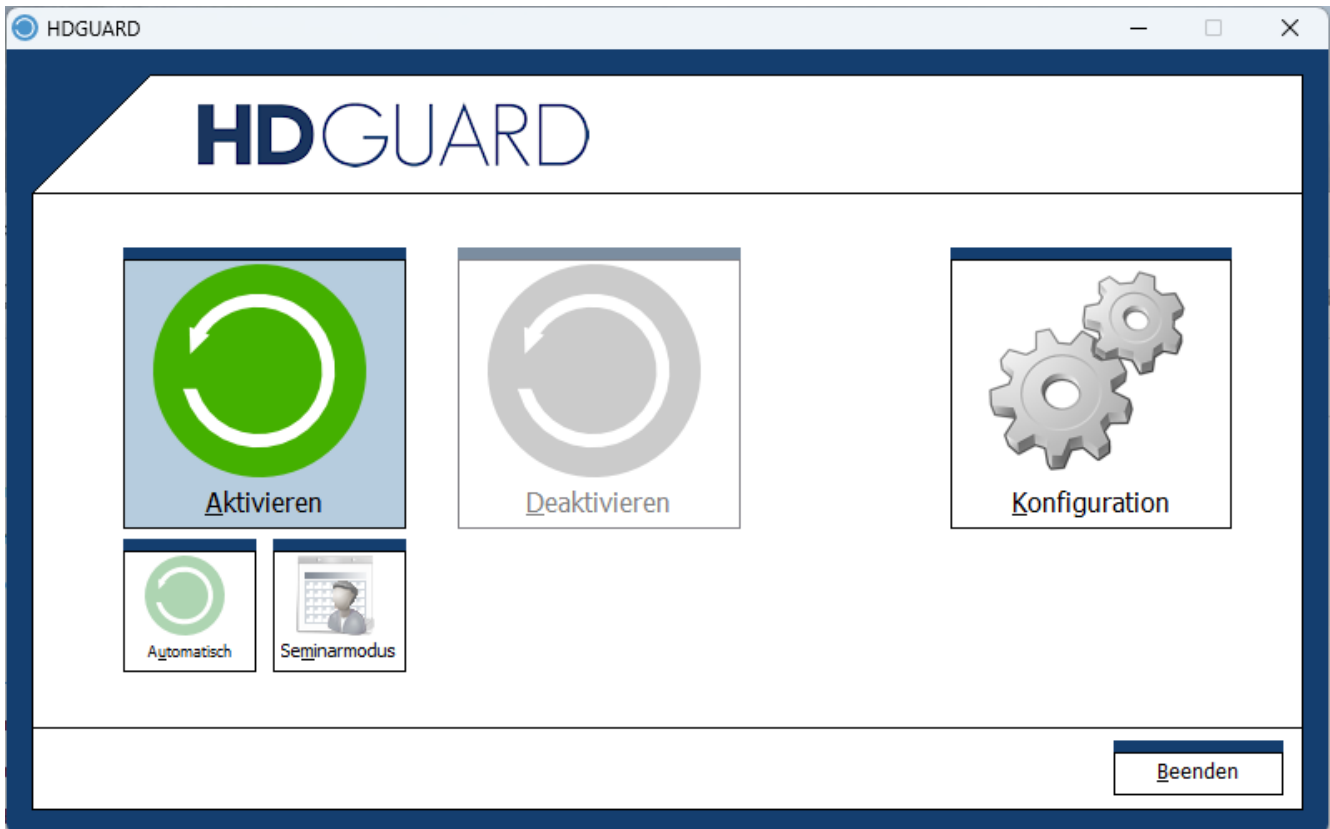
Dieser Konfigurationspunkt zeigt nicht nur Versions- und Lizenzinformationen an, sondern bietet auch die Möglichkeit, die Produktwebseite zu öffnen sowie eine direkte Rückmeldung an die Entwicklung zu geben.



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

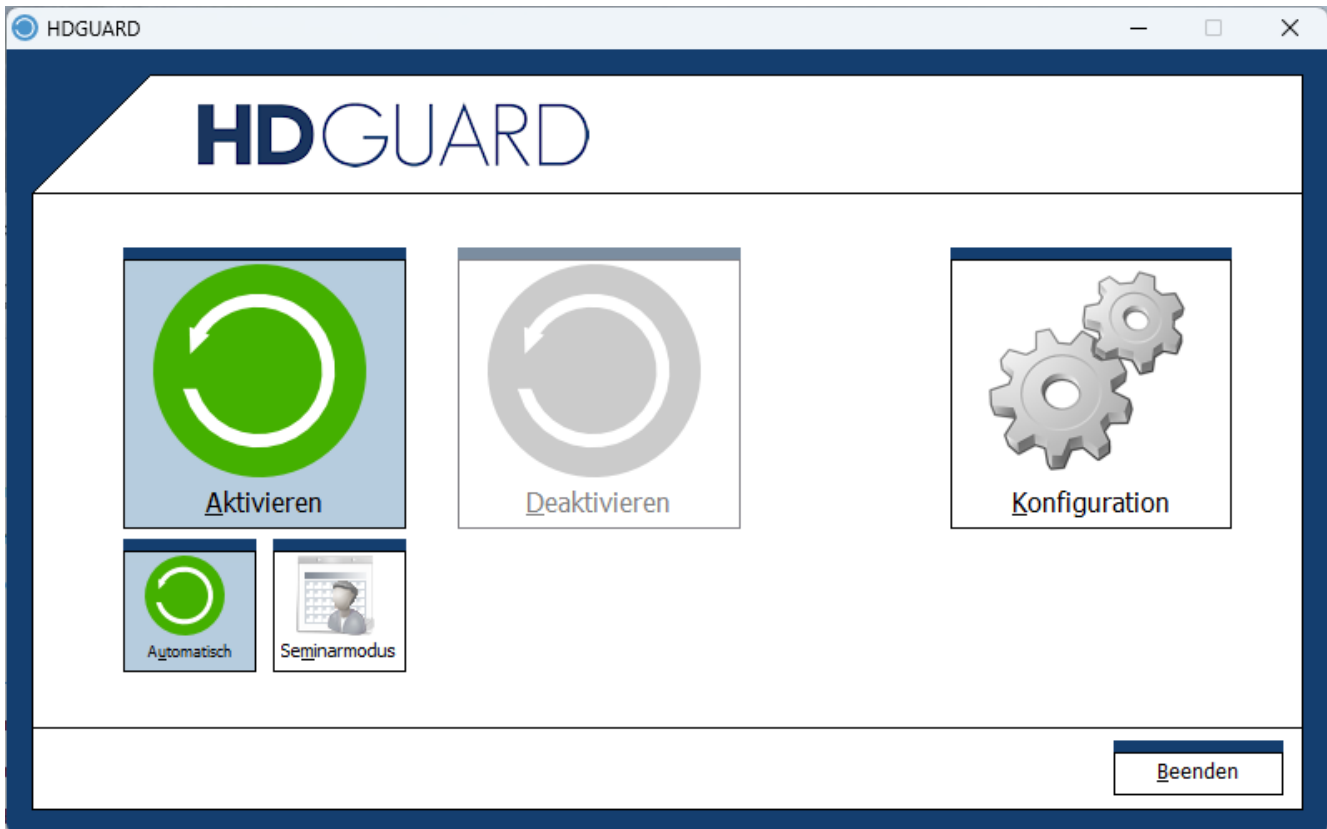
4.3 Hauptfenster

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

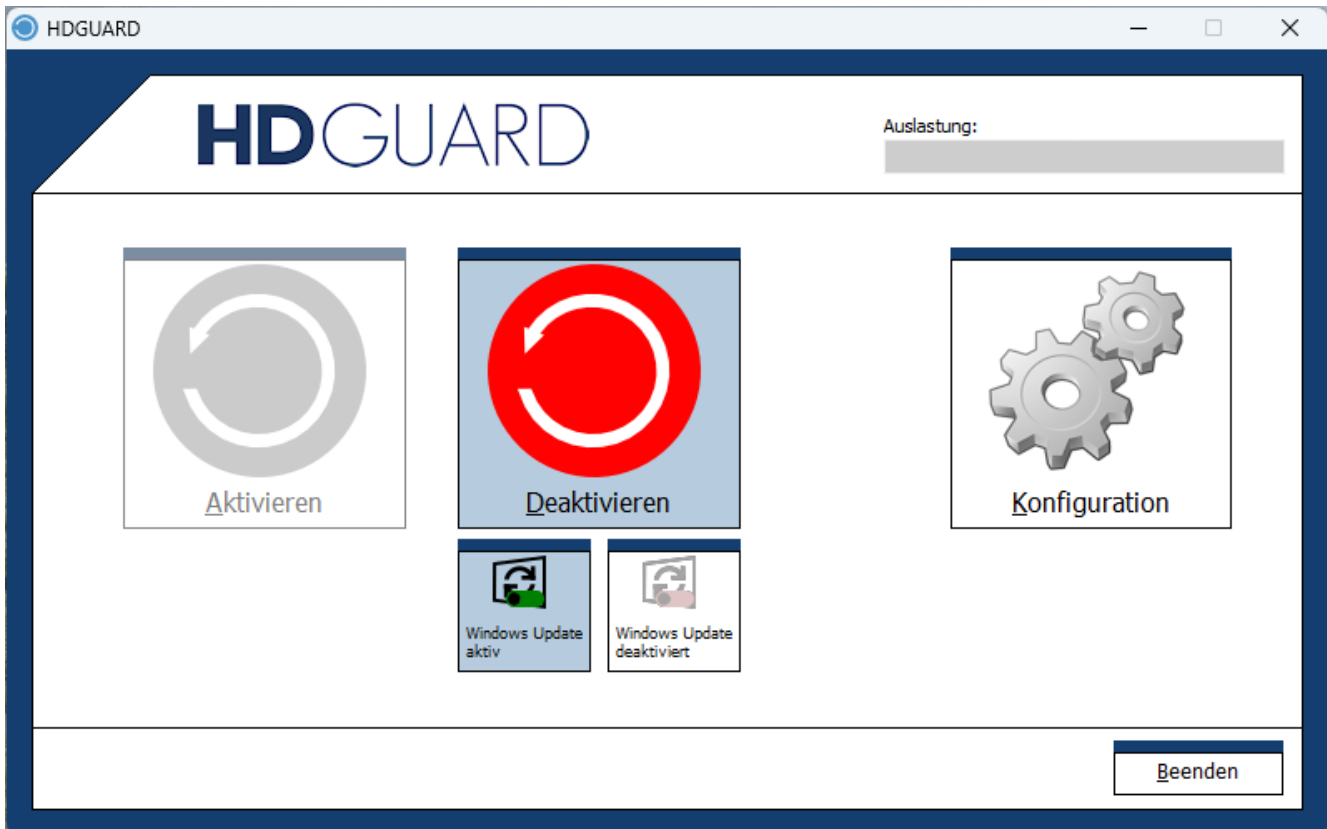
- der Speicherplatz in der jeweiligen HDGUARD SWAP Datei ausgeschöpft ist oder
- ein Benutzer im Kontextmenü des HDGUARD System Tray Icons die Funktion „Seminarmodus zurücksetzen“ auswählt
- eine konfigurierte Rücksetzeinstellung aktiviert ist oder
- ein Updatezeitraum beginnt, dessen Priorität höher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



Beachten Sie bitte die Hinweise zu den Rücksetzeinstellungen des Seminarmodus im Kapitel [Seminarmodus-Rücksetzeinstellungen](#)^[16]

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. Optional ist es möglich Windows Updates nach dem dem Neustart weiterhin zu deaktivieren. Als Standardeinstellung werden nach der Deaktivierung des Schutzes Windows Updates wieder ausgeführt.



Um zu verhindern, dass Windows Updates nach längerem Betrieb im geschützten Modus bei einer Deaktivierung des Schutzes in großer Anzahl nachinstalliert werden, kann die Updatefunktion des Betriebssystems optional inaktiv bleiben.

Wir empfehlen Updatezeiträume, um das System aktuell zu halten.

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 ""
ndwevu7M8gu4/IZgOrznSOETIN7vh9iRU8djZ+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               :Returns 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                     :Returns 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.
/DisableWUAUpem PWD :Leaves automatic Windows Updates disabled when
HDGUARD protection ends.
/EnableWUAUpem PWD :Reenables automatic Windows Updates when HDGUARD
protection is deactivated and the system reboots.
/ExportUSBsticks PWD :Exports a binary file containing the list of all
allowed USB-Sticks into C:\USBstick.bin .
/ImportUSBsticks PWD :Imports the binary file containing the list of
allowed USB-Sticks from C:\USBstick.bin .

```

5.2 Beispiel: ListPartitions

```

C:\Users\Administrator> cd %HDGUARD%
C:\Program Files\IST\HDGUARD>HDGcmd.exe /ListPartitions
-----
HDGUARD index 2
Hard drive 0, partition 1: \\?\Volume{d371bd8f-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\RedirectVolumes

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 per MSI Parameter die Verbindungsdaten übergeben werden.

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

Geänderte Werte werden beim nächsten Neustart des Systems eingelesen. Vergessen Sie nicht, vor diesem Eingriff den HDGUARD Schutz zu deaktivieren!

9 MSI-Parameter

Folgende MSI Parameter werden vom HDGUARD MSI Setup angeboten:

- HDGMASTERNAME : IP oder DNS Name des Systems mit HDGUARD.master Zentralsdienst Installation
- HDGMASTERPORT : vom Standard (52234) abweichender Port beim HDGUARD.master Zentralsdienst.
- INSTALL_TEACHER : Boolescher Wert für die Installation der Lehrerkonsolenkomponente. INSTALL_TEACHER=yes installiert die Lehrerkonsole mit.
- HDGLICENSE : Lizenzschlüssel ohne Bindestriche
- HDGPASSWORD : HDGUARD Passwort

Achten Sie bei den Parametern, insbesondere beim Übergeben des Passworts, darauf, dass die Kommandozeile bestimmte Zeichen als Steuer- und Trennzeichen behandelt und nicht direkt an das aufrufende Programm übergibt.

Der Aufruf für eine unbeaufsichtigte Installation sähe beispielsweise wie folgt aus:

```
msiexec /i HDGUARD12_64.msi /qn HDGMASTERNAME=MyHDGUARDmasterPC  
HDGMASTERPORT=52234 INSTALL_TEACHER=yes
```

10 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.