HDGUARD 13 Referenzhandbuch

Release 13

IST Deutschland GmbH

09.10.2026

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.

HDGUARD ist eine eingetragene Marke der IST Deutschland GmbH.

Microsoft, Windows, Windows Server, Active Directory, Microsoft Defender, Microsoft Store und .NET sind Marken der Microsoft-Unternehmensgruppe. Intel ist eine Marke der Intel Corporation oder ihrer Tochtergesellschaften. AMD64 ist eine Marke von Advanced Micro Devices, Inc. Arm ist eine eingetragene Marke der Arm Limited (oder ihrer Tochtergesellschaften) in den USA und/oder anderen Ländern. Linux ist eine eingetragene Marke von Linus Torvalds in den USA und anderen Ländern. Alle weiteren in diesem Handbuch genannten Firmen- und Produktnamen können Marken der jeweiligen Inhaber sein.

Herausgeber
IST Deutschland GmbH
Bergstraße 23
23843 Neritz

Telefon: +49 4531 8804-40
Support: +49 4531 8804-73
Fax: +49 4531 8804-44
E-Mail: info.de@ist.com
Web: https://www.ist.com/de

HRB 1408, OD Lübeck
Geschäftsführer: Patrik Duda

© 2026 IST Deutschland GmbH

Inhalt

I Grundlagen 1

1 Einführung 2
1.1 HDGUARD . . . 2
1.2 HDGUARD.master . . . 2
1.3 Für wen ist dieses Handbuch? . . . 2
1.4 Aufbau des Handbuchs . . . 3

2 Installation 4
2.1 Art des Schutzes und Einschränkungen . . . 4
2.2 Systemvoraussetzungen . . . 4
2.3 Installation über die Benutzeroberfläche . . . 5
2.4 Aktualisierung . . . 6
2.5 Deinstallation . . . 7
2.6 Installation und Einrichtung eines Multiboot-Systems . . . 7

3 Lizenzierung und Testzeitraum 8
3.1 Testzeitraum . . . 8
3.2 Lizenzschlüssel und Software-Aktivierung . . . 8
3.3 Abgelaufene oder ungültige Lizenz . . . 8

II Erste Einrichtung 10

4 Die Bedienoberfläche im Überblick 11
4.1 Programmstart . . . 11
4.2 Anmeldung . . . 11
4.3 Das Hauptfenster . . . 12
4.4 Meldungsleisten . . . 13
4.5 Gesperrtes Fenster bei laufenden Vorgängen . . . 13

5 Schritt für Schritt zum aktiven Schutz 14
5.1 HDGUARD zum ersten Mal starten . . . 14
5.2 Internetverbindung einrichten (nur mit Proxyserver) . . . 15
5.3 Lizenzschlüssel eingeben und Software aktivieren . . . 15
5.4 HDGUARD-Passwort setzen . . . 15
5.5 Festplatten automatisch zuweisen . . . 15
5.6 Update-Zeitraum einrichten (optional) . . . 16
5.7 Schutz aktivieren . . . 17
5.8 Nach dem Neustart . . . 17

6 Im laufenden Betrieb 18
6.1 Was bei aktivem Schutz gilt . . . 18
6.2 Software installieren oder Einstellungen dauerhaft ändern . . . 18
6.3 Meldungen im Betrieb . . . 18
6.4 Darstellung der Oberfläche anpassen . . . 19

© 2026 IST Deutschland GmbH

III Weitere Einstellungen und Expertenansicht 20

7 Die Expertenansicht 21
7.1 Expertenansicht einschalten . . . 21
7.2 Was die Expertenansicht zusätzlich bietet . . . 21

8 Schutz aktivieren und deaktivieren 22
8.1 Schutz aktivieren . . . 22
8.2 Multiboot-Systeme . . . 23
8.3 Seminar-Modus . . . 24
8.4 Schutz deaktivieren . . . 25
8.5 Windows Update und Schutz . . . 25

9 Festplatten 26
9.1 Darstellung . . . 26
9.2 Schutzmodi je Partition . . . 27
9.3 Vollständige Konfiguration . . . 27
9.4 Automatisch zuweisen . . . 27
9.5 Partitionen einzeln konfigurieren . . . 28

10 Passwörter 29
10.1 HDGUARD-Passwort setzen, ändern oder entfernen . . . 29
10.2 Seminar-Passwort . . . 29
10.3 Anmeldung ohne Passworteingabe . . . 30

11 Sichtbarkeiten 31
11.1 Verknüpfungen . . . 31
11.2 Benutzeroberfläche . . . 31

12 Lizenzierung 33
12.1 Lizenzschlüssel eingeben . . . 33
12.2 Software-Aktivierung über das Internet . . . 33
12.3 Offline Software-Aktivierung . . . 34
12.4 Lizenz zurücksetzen . . . 34
12.5 Lizenz wechseln . . . 34
12.6 Lizenzinformationen . . . 34

13 Internet-Einstellungen 36
13.1 Verbindungsart . . . 36

14 Update-Zeiträume 37
14.1 Zeiträume . . . 37
14.2 Ablauf eines Update-Zeitraums . . . 38
14.3 Spezielle Update-Zeiträume . . . 39

15 USB-Sticks 40
15.1 Behandlung der lokalen USB-Massenspeicher . . . 40
15.2 Zugelassene USB-Massenspeicher . . . 40

16 Ausnahmen 42
16.1 Ausnahmeziel festlegen . . . 42
16.2 Registry-Ausnahmen . . . 43
16.3 Verzeichnisverbindungen auf C: . . . 43

17 HDGUARD.master 44
17.1 Verbindung einrichten . . . 44
17.2 Benachrichtigungen für angemeldete Benutzer . . . 45

© 2026 IST Deutschland GmbH

18 Info und Einstellungen **46**
18.1 Einstellungen 46
18.2 Info 46

IV Automatisierung und Referenz 47

19 Bedienung per Kommandozeile **48**
19.1 Verschlüsselte Passwörter 48
19.2 Befehle 48

20 Klonen **54**
20.1 Installation in einen Klon-Master 54
20.2 Automatische Einrichtung nach dem Klonen 54

21 Unbeaufsichtigte Installation (MSI-Parameter) **56**

22 Lehrerkonsole **58**

23 Ereignisprotokoll **59**
23.1 HDGUARD Service 59
23.2 RDTserv 63

24 Glossar **64**

Stichwortverzeichnis **66**

© 2026 IST Deutschland GmbH

Teil I

Grundlagen

© 2026 IST Deutschland GmbH

Kapitel 1

Einführung

1.1 HDGUARD

HDGUARD® schützt Ihre Festplatten vor dauerhaften Veränderungen. Nach einem *Neustart* des PCs wird automatisch der gewünschte Originalzustand wiederhergestellt. Selbst wenn 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 dies dadurch, dass HDGUARD alle Veränderungen an den konfigurierten Partitionen entweder unterbindet oder in *Swap-Dateien* umleitet. Zur Laufzeit des Betriebssystems können alle Funktionen ohne Einschränkungen genutzt werden; der Anwender erkennt keinen Unterschied zu einem herkömmlichen, ungeschützten PC. Sobald der PC neu gestartet wird, verwirft HDGUARD alle Änderungen. Dafür wird nur ein Bruchteil einer Sekunde benötigt, egal wie umfangreich die Änderungen waren.

Abgerundet wird die Funktionalität durch einen wirkungsvollen USB-Schutz, der die Nutzung von USB-Laufwerken einschränkt. Zahlreiche Optionen stellen sicher, dass sich HDGUARD gut in bestehende IT-Konzepte integrieren lässt – etwa *Update-Zeiträume* für automatische Updates von Microsoft® Windows®, die zentrale Verwaltung über *HDGUARD.master* und die Steuerung per *Kommandozeile*.

HDGUARD ist eine reine Softwarelösung. Es sind keine Eingriffe in die Hardware der geschützten Systeme erforderlich. Durch den Verzicht auf PC-Karten oder Dongles fügt sich HDGUARD in neue wie in bestehende Systeme ein.

1.2 HDGUARD.master

HDGUARD.master zentralisiert die Steuerung und Überwachung der HDGUARD-geschützten PCs in Ihrem Netzwerk. Deaktivieren Sie gezielt einzelne PCs oder ganze Räume, überwachen Sie automatisch den Schutz Ihrer PCs und lassen Sie Sicherheitswarnungen erscheinen, wenn ein PC ungeschützt hochgefahren ist. Darüber hinaus bietet HDGUARD.master didaktische Funktionen, etwa über die *Lehrerkonsole*.

Näheres finden Sie im Handbuch zu HDGUARD.master. Wie ein HDGUARD-PC mit HDGUARD.master verbunden wird, beschreibt *HDGUARD.master*.

1.3 Für wen ist dieses Handbuch?

Wer HDGUARD bedient, verwaltet damit zugleich den Schutz des PCs. Dieses Handbuch beschreibt deshalb die Bedienung und die Verwaltung gemeinsam – von der Installation über die Konfiguration bis zur automatisierten Einrichtung vieler PCs.

© 2026 IST Deutschland GmbH

1.4 Aufbau des Handbuchs

Teil I – Grundlagen
Was HDGUARD leistet, die *Installation* und das *Lizenzmodell* mit Testzeitraum und Software-Aktivierung.

Teil II – Erste Einrichtung
Ein Rundgang durch die *Bedienoberfläche* und die *erste Einrichtung Schritt für Schritt* – so, wie Sie sie am PC erleben: vom ersten Start bis zum aktiven Schutz. Danach der *laufende Betrieb*, etwa das Deaktivieren des Schutzes für Wartungsarbeiten. Dieser Teil kommt ohne die Expertenansicht aus.

Teil III – Weitere Einstellungen und Expertenansicht
Jeder Bereich der Oberfläche noch einmal vollständig – mit allen Einstellungen der *Expertenansicht*, etwa Seminar-Modus, einzelne Partitionen, USB-Sticks, Ausnahmen und HDGUARD.master.

Teil IV – Automatisierung und Referenz
Kommandozeile, *Klonen* und *unbeaufsichtigte Installation*, dazu die Einträge im *Ereignisprotokoll* und das *Glossar*.

© 2026 IST Deutschland GmbH

Kapitel 2

Installation

Warnung
Fertigen Sie vor der Installation 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 IST Deutschland GmbH und ihre Partner haften nicht für eventuelle Datenverluste und deren Folgen.

Wichtig
Sollen HDGUARD und (Teile von) *HDGUARD.master* auf demselben System installiert werden, muss HDGUARD.master zuerst installiert werden.

2.1 Art des Schutzes und Einschränkungen

HDGUARD schützt die Daten auf der Festplatte grundsätzlich **per Partition**. Alle Änderungen an Dateien und Registry-Einträgen auf einer geschützten Partition – insbesondere auf dem Systemlaufwerk `C:` – werden durch einen Neustart zurückgesetzt. Für bestimmte Szenarien bietet HDGUARD Hilfsfunktionen, die diese Einschränkung abmildern:

- *Update-Zeiträume*, um bei zeitweise deaktiviertem Schutz Updates einzuspielen (empfohlen),
- in seltenen Fällen *Ausnahmen*. Dafür ist eine zusätzliche Partition auf der Systemfestplatte notwendig, die sich auch nachträglich anlegen lässt.

Bei aktivem Schutz ist Windows Update abgeschaltet. Updates für Windows und Microsoft Defender lassen sich nur bei deaktiviertem Schutz oder in einem Update-Zeitraum installieren. Außerdem ist die Funktionalität des Microsoft Store bei aktivem Schutz eingeschränkt.

2.2 Systemvoraussetzungen

Hardware
: Handelsüblicher PC mit x64-Prozessorarchitektur (Intel® 64 bzw. AMD64™) oder ARM64-Prozessorarchitektur.

TPM
: TPM 2.0 (diskret, Firmware-TPM oder virtuelles TPM), in der Firmware aktiviert und von Windows als einsatzbereit erkannt. Kann das Setup keine *Gerätekennung* aus dem TPM lesen, bricht es die Installation ab.

Betriebssystem
: **x64** (Intel 64, AMD64): Microsoft Windows 10 ab Version 2004, Microsoft Windows 11, Windows Server 2022 und Windows Server 2025.

  ARM64: Microsoft Windows 11. Für Geräte mit ARM64-Prozessorarchitektur gibt es ein eigenes Setup.

© 2026 IST Deutschland GmbH

Software
Microsoft .NET Framework 4.8 oder neuer bei Nutzung der Lehrerkonsole.

Arbeitsspeicher
Mindestens 4 GB RAM (empfohlen mindestens 8 GB)

Festplatte
128 GB Festplatte, SSHD oder SSD (empfohlen mindestens 180 GB).

MBR oder GPT mit primären und sekundären Partitionen. Die Windows-Startkonfiguration muss intakt sein.

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

Partitionszusammenführungen wie dynamische Datenträger werden nicht unterstützt.

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

Andere Schutzsoftware
Andere Festplattenschutz- oder Wiederherstellungssoftware sollte nicht installiert sein. Das Setup warnt in diesem Fall.

2.3 Installation über die Benutzeroberfläche

1. Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
2. Starten Sie die für Ihre Plattform passende MSI-Datei. Die aktuellen Installationsquellen erhalten Sie im Internet unter https://www.ist.com/de/downloads.
3. Folgen Sie dem Installationsassistenten.
4. Starten Sie den PC nach Abschluss der Installation neu.

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

© 2026 IST Deutschland GmbH

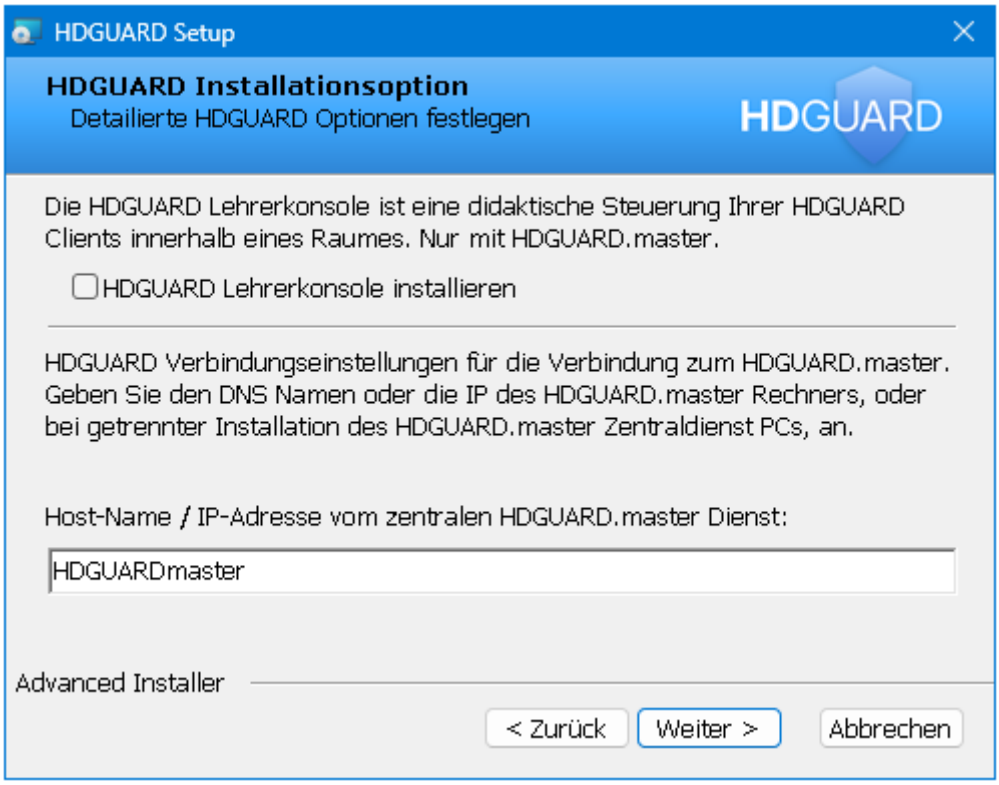


Abb. 2.1: Setup-Dialog „HDGUARD Installationsoption“

Im Dialog **HDGUARD Installationsoption** (Abb. 2.1) legen Sie fest:

HDGUARD Lehrerkonsole installieren
: Die *Lehrerkonsole* funktioniert nur zusammen mit HDGUARD.master und sollte nur an Arbeitsplätzen installiert werden, an denen Dozenten arbeiten.

Host-Name / IP-Adresse vom zentralen HDGUARD.master Dienst
: Ohne besondere Einstellung wird `HDGUARDmaster` verwendet. Das ist richtig, wenn der PC mit dem zentralen HDGUARD.master-Dienst so heißt oder ein entsprechender Alias im DNS eingetragen ist – und ebenso für Umgebungen ohne HDGUARD.master. Andernfalls tragen Sie den Namen oder die IP-Adresse dieses PCs ein.

Im anschließenden Dialog **Telemetrie** entscheiden Sie, ob HDGUARD Konfigurationsdaten übermitteln darf (siehe *Telemetrie*).

HDGUARD wird nach `C:\Program Files\IST\HDGUARD` installiert.

Für die unbeaufsichtigte Installation siehe *Unbeaufsichtigte Installation (MSI-Parameter)*, für die Installation in ein Master-Image *Installation in einen Klon-Master*.

2.4 Aktualisierung

Das Setup von HDGUARD 13 aktualisiert vorhandene Installationen ab HDGUARD 12 direkt. Starten Sie dazu das jeweilige Setup wie bei einer Neuinstallation.

Ist eine neue HDGUARD-Version verfügbar, meldet das Hauptfenster das beim Start mit „Eine neue HDGUARD-Version ist verfügbar.“ Bei ausgeschaltetem Schutz enthält die Meldungsleiste die Schaltfläche **Updater starten**; sie schließt HDGUARD und startet die Aktualisierung.

> **Wichtig**
> Deaktivieren Sie vor jeder Aktualisierung den Schutz. Bei aktivem Schutz bricht das Setup ab.

© 2026 IST Deutschland GmbH

2.5 Deinstallation

Deaktivieren Sie zunächst den *Schutz*. Deinstallieren Sie HDGUARD anschließend über die Windows-Einstellungen (**Apps**) bzw. **Programme und Features**.

Sie haben die Möglichkeit, die Konfiguration bei der Deinstallation zu löschen, wenn Sie die entsprechende Option im Dialog aktivieren. Dann wird im Folgefenster das aktuelle HDGUARD-Passwort abgefragt.

> **Wichtig**
> Der Neustart nach der Deinstallation ist zwingend erforderlich, bevor weitere Aktionen durchgeführt werden.

2.6 Installation und Einrichtung eines Multiboot-Systems

HDGUARD unterstützt Multiboot-Systeme mit dem Windows-Bootmanager. Die Einrichtung beginnt bereits mit der Partitionierung vor der Installation von Windows – lesen Sie deshalb vorher *Multiboot-Systeme*.

© 2026 IST Deutschland GmbH

Kapitel 3

Lizenzierung und Testzeitraum

3.1 Testzeitraum

Nach der Installation können Sie HDGUARD **30 Tage** lang ohne Lizenzschlüssel testen. Im Testzeitraum stehen alle Funktionen zur Verfügung – mit Ausnahme der *Passwörter* und der *Sichtbarkeiten*. Das Hauptfenster weist mit einer Meldungsleiste darauf hin.

Das Ende des Testzeitraums zeigt die Ansicht **Lizenzierung** an, z. B. „Testzeitraum endet am 15.10.2026 (noch 12 Tage)."

3.2 Lizenzschlüssel und Software-Aktivierung

Für den dauerhaften Betrieb sind zwei Schritte erforderlich:

1. die Eingabe eines gültigen **Lizenzschlüssels** und
2. die Registrierung der Installation bei IST Deutschland, die **Software-Aktivierung**.

Nach der Eingabe des Lizenzschlüssels steht Ihnen die volle Funktionalität zunächst für eine begrenzte Zeit zur Verfügung. Bis wann die Software-Aktivierung erfolgen muss, zeigt die Ansicht **Lizenzierung**: „Die Software-Aktivierung muss bis zum … erfolgen."

Bei der Software-Aktivierung wird ein Datenpaket aus Lizenzschlüssel und *Gerätekennung* an einen Server von IST Deutschland übertragen. Die Antwort schaltet die Installation für die Länge der aktuellen Subskriptionsperiode frei und enthält zugleich aktualisierte Lizenzinformationen. Die Verbindung ist nach aktuellem Stand der Technik verschlüsselt.

> ⚠ **Warnung**
> Wird der TPM-Chip nach der Installation in den Firmware-Einstellungen des PCs deaktiviert, kann HDGUARD die Software-Aktivierung weder durchführen noch überprüfen. In diesem Fall wird ein Fehler angezeigt und es gilt Abschnitt 3.3.

HDGUARD frischt die Software-Aktivierung regelmäßig selbstständig über das Internet auf, damit die Lizenzinformationen aktuell bleiben. Für alle Verbindungen zum Aktivierungsserver gelten die *Internet-Einstellungen*.

Wie Sie den Lizenzschlüssel bei der ersten Einrichtung eingeben und die Software sofort aktivieren, beschreibt *Lizenzschlüssel eingeben und Software aktivieren*; alle Möglichkeiten der Ansicht – auch die Aktivierung ohne Internetverbindung – beschreibt das Kapitel *Lizenzierung*.

3.3 Abgelaufene oder ungültige Lizenz

Ist die Lizenz oder Software-Aktivierung nicht in Ordnung, gilt: „HDGUARD kann nicht vollständig genutzt werden. Es kann nur noch der Schutz deaktiviert werden."

- **Schutz aktivieren** ist gesperrt.
- Die Bereiche **Sichtbarkeit**, **Update-Zeiträume**, **USB**, **Ausnahmen** und **HDGUARD.master** stehen nicht zur Verfügung.

© 2026 IST Deutschland GmbH

⚠ Warnung
Ist der Schutz aktiv, während Lizenz oder Software-Aktivierung nicht in Ordnung ist, fährt HDGUARD den PC 20 Minuten nach der Benutzeranmeldung herunter. Eine Meldung „HDGUARD Lizenzproblem“ kündigt das an: „Lizenz oder Software-Aktivierung ist nicht in Ordnung! Das System wird innerhalb von 20 Minuten heruntergefahren!“ Ist der Testzeitraum abgelaufen, weist die Meldung stattdessen auf das Ende des Testzeitraums hin. Führen Sie die Lizenzierung deshalb rechtzeitig vor Ablauf der Fristen durch.

© 2026 IST Deutschland GmbH

Teil II

Erste Einrichtung

© 2026 IST Deutschland GmbH

Kapitel 4

Die Bedienoberfläche im Überblick

Dieses Kapitel zeigt, wie die HDGUARD-Oberfläche aufgebaut ist. Wie Sie HDGUARD damit zum ersten Mal einrichten, führt das nächste Kapitel *Schritt für Schritt zum aktiven Schutz* Schritt für Schritt durch. Beschrieben wird die **Standardansicht**; die zusätzlichen Bereiche der *Expertenansicht* folgen in Teil III.

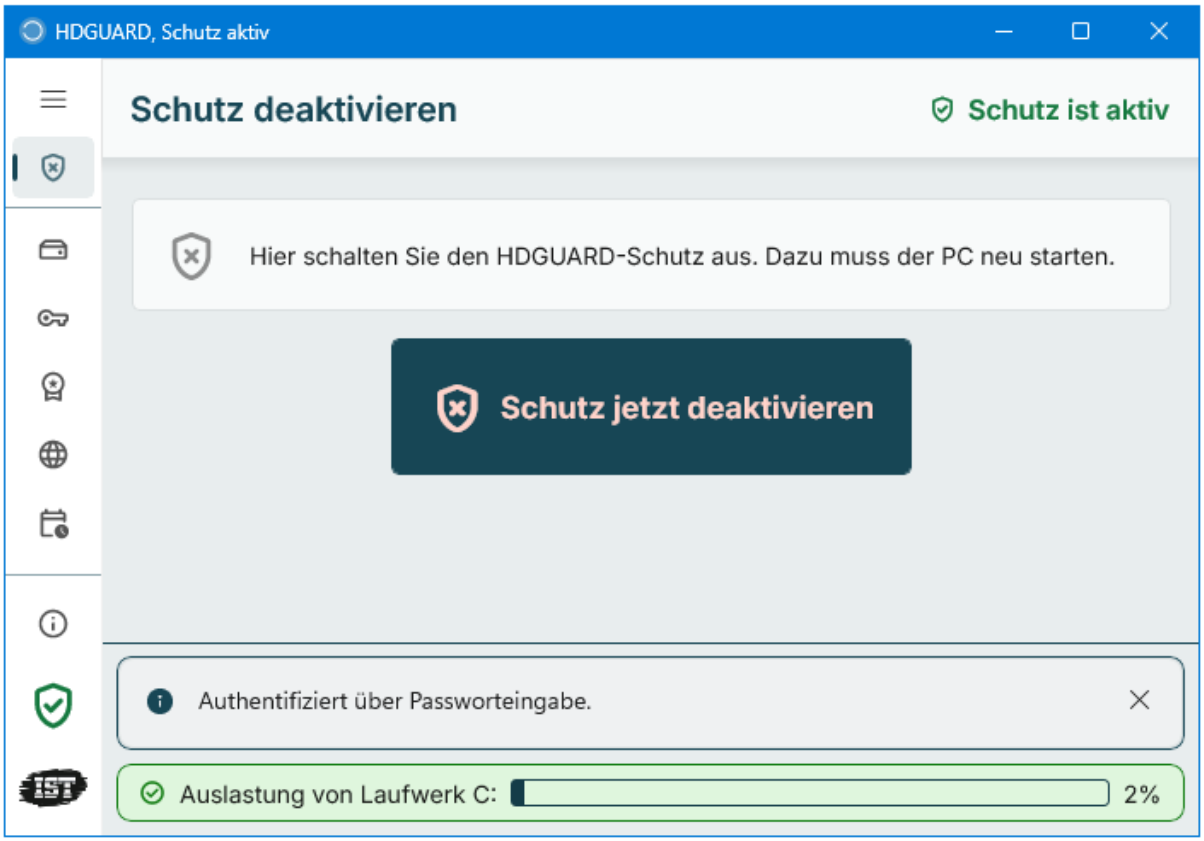


Abb. 4.1: Das Hauptfenster bei aktivem Schutz (Menü eingeklappt)

4.1 Programmstart

Nach der Installation finden Sie HDGUARD im Windows-Startmenü, auf dem Desktop und im Infobereich der Taskleiste.

4.2 Anmeldung

Ist kein HDGUARD-Passwort gesetzt, öffnet sich die Oberfläche ohne Anmeldung. Ist ein Passwort gesetzt, erscheint der Dialog **Bei HDGUARD anmelden**:

1. Geben Sie das **HDGUARD-Passwort** ein.
2. Klicken Sie auf **Anmelden** oder drücken Sie `Eingabe`.

© 2026 IST Deutschland GmbH

Unter „Andere Anmeldeoptionen“ bietet der Dialog zusätzlich an, sofern verfügbar:

- **Admin-Stick Anmeldung** – wenn ein angelernter *Admin-Stick* angeschlossen ist,
- **Domänengruppen Anmeldung** – wenn der angemeldete Benutzer Mitglied der Domänengruppe „HDGUARD-Administrators“ ist.

Beide Anmeldearten stehen erst zur Verfügung, wenn sie eingerichtet sind – und das geschieht nicht in der Standardansicht: Admin-Sticks lernen Sie in der Ansicht *USB* an, die nur in der *Expertenansicht* sichtbar ist; die Domänengruppe wird in der Domäne (Active Directory) angelegt. Details zu beiden Anmeldearten finden Sie unter *Passwörter*.

Nach **drei** falschen Passworteingaben sperrt die Oberfläche den Zugang („Zugang verweigert“) und muss mit **Beenden** geschlossen werden.

> ⚠ **Warnung**
> Bewahren Sie das HDGUARD-Passwort sorgfältig auf. Es gibt keine fest einprogrammierten Passwörter und keine Möglichkeit, ein vergessenes Passwort wiederherzustellen.

Nach der Anmeldung zeigt eine Meldungsleiste, wie Sie angemeldet sind, z. B. „Authentifiziert über Passworteingabe.“ Unter *Info & Einstellungen* lässt sich einstellen, dass dieser Hinweis nach fünf Sekunden automatisch verschwindet.

4.3 Das Hauptfenster

Das Hauptfenster (Abb. 4.1) besteht aus

- dem **Menü** am linken Rand, das sich ein- und ausklappen lässt,
- dem **Seitenkopf** mit dem Titel der gewählten Ansicht,
- dem **Inhaltsbereich** der gewählten Ansicht und
- den **Meldungsleisten** am unteren Rand, die auf Zustände und erforderliche Aktionen hinweisen.

4.3.1 Statusanzeige

Der Kopf des Menüs zeigt, ob der Schutz eingeschaltet ist: **Schutz aktiv** bzw. **Schutz inaktiv**. Bei eingeklapptem Menü erscheint der Status als Symbol am unteren Menürand und im Seitenkopf („Schutz ist aktiv“ / „Schutz ist inaktiv“).

Auch der Fenstertitel nennt den Zustand: „HDGUARD, Schutz aktiv“ bzw. „HDGUARD, Seminar-Modus aktiv“.

4.3.2 Das Menü

Welche Einträge das Menü zeigt, hängt vom Schutzzustand, der Lizenz und der *Expertenansicht* ab.

4.3.3 Standardansicht und Expertenansicht

Am unteren Menürand schaltet **Expertenansicht** zusätzliche Bereiche und Einstellungen ein. Für die erste Einrichtung und den normalen Betrieb wird sie nicht benötigt. Was sie bietet, beschreibt *Die Expertenansicht*.

© 2026 IST Deutschland GmbH

4.4 Meldungsleisten

Am unteren Rand des Hauptfensters erscheinen Meldungsleisten, unter anderem

- zum Lizenzstatus – solange die Lizenzierung nicht abgeschlossen ist, mit Sprung in die Ansicht **Lizenzierung**,
- wenn kein HDGUARD-Passwort gesetzt ist („Diese HDGUARD-Installation ist nicht durch ein HDGUARD-Passwort geschützt.“), mit Sprung in die Ansicht **Passwort**,
- zur Auslastung der *Swap-Datei* bei aktivem Schutz (grün bis 50 %, gelb bis 80 %, darüber rot),
- zu laufenden *Update-Zeiträumen*,
- zur *Windows Update Sperre*, z. B. „Windows Update benötigt einen Neustart des PCs. Der HDGUARD Schutz kann daher nicht aktiviert werden.“,
- wenn eine neue HDGUARD-Version verfügbar ist (siehe *Aktualisierung*).

Meldungen, die eine Aktion erfordern, lassen sich nicht schließen, bis die Ursache behoben ist.

4.5 Gesperrtes Fenster bei laufenden Vorgängen

Während das Aktivieren oder Deaktivieren des Schutzes läuft, ist das Fenster gesperrt; auch das Schließen und das Herunterfahren von Windows werden blockiert. Die Sperre endet mit dem Neustart des PCs.

© 2026 IST Deutschland GmbH

Kapitel 5

Schritt für Schritt zum aktiven Schutz

Dieses Kapitel führt Sie durch die erste Einrichtung – in der Reihenfolge, in der Sie sie am PC erleben: vom ersten Start der Oberfläche bis zum aktiven Schutz. Alle Schritte gelingen in der Standardansicht.

5.1 HDGUARD zum ersten Mal starten

Starten Sie HDGUARD nach der Installation und dem anschließenden Neustart über das Startmenü oder die Desktop-Verknüpfung. Da noch kein Passwort gesetzt ist, öffnet sich die Oberfläche ohne Anmeldung.

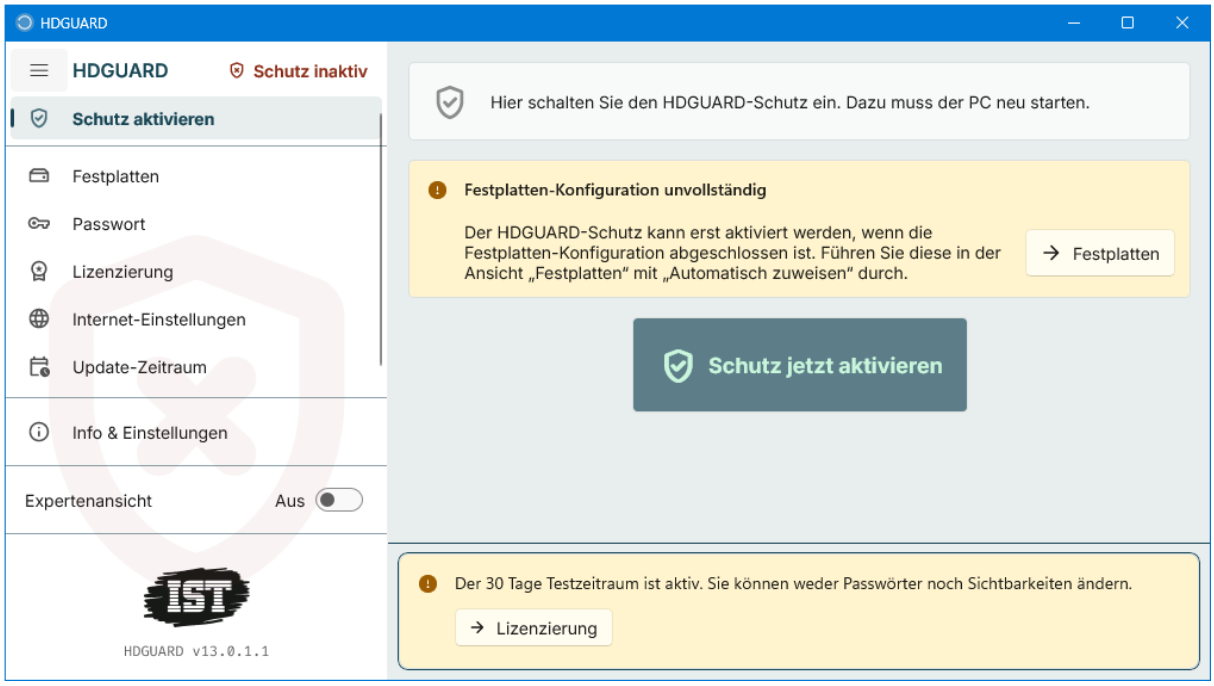


Abb. 5.1: Das Hauptfenster beim ersten Start

Die Ansicht **Schutz aktivieren** zeigt, dass die Festplatten-Konfiguration noch fehlt; der Schutz lässt sich deshalb noch nicht einschalten. Die Meldungsleiste am unteren Rand weist auf den Testzeitraum hin.

> **Bemerkung**
> Möchten Sie HDGUARD zunächst nur **testen**, überspringen Sie die Lizenzierung und das Passwort – im Testzeitraum lässt sich kein Passwort setzen. *Festplatten zuweisen* und *Schutz aktivieren* funktionieren auch ohne Lizenzschlüssel.

© 2026 IST Deutschland GmbH

5.2 Internetverbindung einrichten (nur mit Proxyserver)

Für die Lizenzierung braucht HDGUARD eine Internetverbindung. Erreicht der PC das Internet direkt, überspringen Sie diesen Schritt.

1. Klicken Sie im Menü auf **Internet-Einstellungen**.
2. Wählen Sie **Internetverbindung über Proxyserver**.
3. Geben Sie **Proxy-Adresse** und **Port** ein, bei Bedarf auch Benutzername und Passwort.
4. Klicken Sie auf **Speichern**.

5.3 Lizenzschlüssel eingeben und Software aktivieren

1. Klicken Sie im Menü auf **Lizenzierung** – oder auf die Schaltfläche in der Meldungsleiste.
2. Klicken Sie auf **Setzen**, geben Sie den 20-stelligen Lizenzschlüssel ein und bestätigen Sie mit **OK**.
3. Klicken Sie auf **Software-Aktivierung**. HDGUARD bestätigt die erfolgreiche Aktivierung.

Kann der PC den Aktivierungsserver nicht erreichen, öffnet sich der Dialog **Offline Software-Aktivierung** (siehe *Offline Software-Aktivierung*).

5.4 HDGUARD-Passwort setzen

Solange kein Passwort gesetzt ist, kann jeder Benutzer HDGUARD öffnen und den Schutz abschalten.

1. Klicken Sie im Menü auf **Passwort** – oder auf die Schaltfläche in der Meldungsleiste.
2. Klicken Sie auf **Setzen**.
3. Geben Sie das neue Passwort zweimal ein (höchstens 16 Zeichen) und bestätigen Sie mit **OK**.

> **⚠ Warnung**
> Notieren Sie das Passwort und bewahren Sie es sicher auf. Ein vergessenes Passwort lässt sich nicht wiederherstellen.

5.5 Festplatten automatisch zuweisen

1. Klicken Sie im Menü auf **Festplatten**.
2. Klicken Sie auf **Automatisch zuweisen**.

Die Karte **Festplatten-Konfiguration** meldet danach, dass die Konfiguration vollständig ist (Abb. 5.2).

© 2026 IST Deutschland GmbH

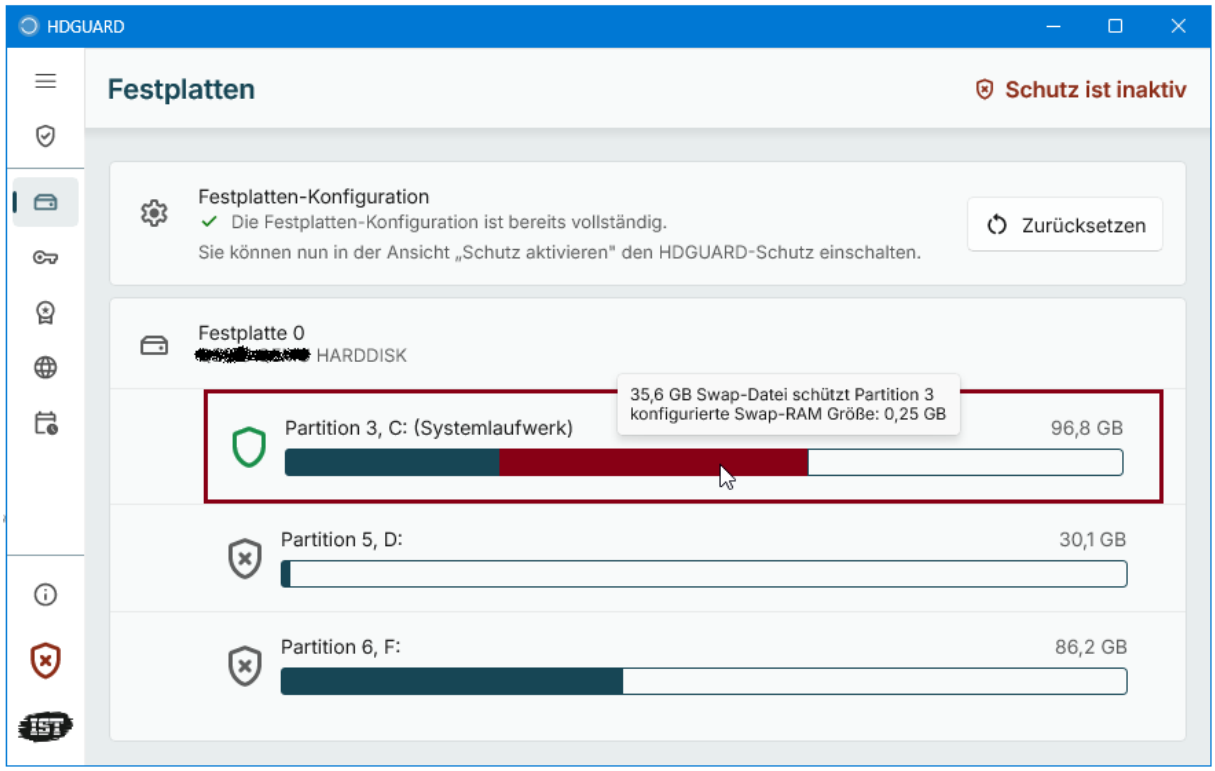


Abb. 5.2: Die Ansicht „Festplatten“ nach „Automatisch zuweisen“

Schlägt die automatische Zuweisung fehl, starten Sie den PC neu und versuchen Sie es erneut. Ist sie grundsätzlich nicht möglich, konfigurieren Sie die Partitionen einzeln in der Expertenansicht (siehe *Festplatten*).

5.6 Update-Zeitraum einrichten (optional)

> **Bemerkung**
> Dieser Schritt ist **optional**. Sie können ihn überspringen und jederzeit später nachholen.

Bei aktivem Schutz ist Windows Update abgeschaltet. Mit einem *Update-Zeitraum* installiert HDGUARD Windows-Updates trotzdem regelmäßig, ohne dass Sie den Schutz von Hand abschalten müssen.

1. Klicken Sie im Menü auf **Update-Zeitraum**.
2. Schalten Sie **Zeitraum 1** ein.
3. Drücken Sie dann auf die Schaltfläche **Windows Update durchführen**.
4. Legen Sie **Minimum-Dauer (Minuten)** und **Startzeit** fest und wählen Sie **Täglich ausführen** oder einzelne Tage. Dauert die Installation der Updates länger, verlängert HDGUARD den Zeitraum automatisch.
5. Klicken Sie auf **Speichern**.

Die Experteneinstellungen und weitere Arten von Update-Zeiträumen beschreibt *Update-Zeiträume*.

© 2026 IST Deutschland GmbH

5.7 Schutz aktivieren

1. Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
2. Klicken Sie im Menü auf **Schutz aktivieren** und dann auf **Schutz jetzt aktivieren**.
3. Bestätigen Sie die Rückfrage mit **Ja**.

HDGUARD bereitet Windows unmittelbar auf den Schutz vor und startet den PC anschließend von selbst neu.

> **Bemerkung**
> Wartet Windows Update noch auf einen Neustart, lässt sich der Schutz nicht aktivieren – starten Sie den PC dann zuerst neu.

5.8 Nach dem Neustart

Der PC startet mit aktivem Schutz. Ohne weitere Einstellung weist beim Anmelden eines Benutzers an Windows ein HDGUARD-Hinweisfenster auf den aktiven Schutz hin; es lässt sich unter *Sichtbarkeiten* abschalten.

Öffnen Sie HDGUARD jetzt, fragt die Oberfläche ggf. nach dem Passwort und zeigt den aktiven Schutz an (Abb. 4.1).

Damit ist die Einrichtung abgeschlossen: Jeder Neustart setzt den PC auf den Zustand beim Einschalten des Schutzes zurück. Wie Sie Software installieren oder Einstellungen dauerhaft ändern, beschreibt *Im laufenden Betrieb*.

© 2026 IST Deutschland GmbH

Kapitel 6

Im laufenden Betrieb

6.1 Was bei aktivem Schutz gilt

- Jeder *Neustart* setzt die geschützten Partitionen auf den Zustand zurück, den sie beim Aktivieren des Schutzes hatten. Was Benutzer in der Zwischenzeit installieren, ändern oder löschen, ist danach verworfen.
- Windows Update ist abgeschaltet. Updates können nur in einem *Update-Zeitraum* oder bei deaktiviertem Schutz installiert werden.
- Einstellungen, die den Schutz selbst betreffen – etwa die *Festplatten* oder die *Internet-Einstellungen* –, lassen sich nur bei ausgeschaltetem Schutz ändern.

6.2 Software installieren oder Einstellungen dauerhaft ändern

Soll eine Änderung dauerhaft erhalten bleiben – etwa eine neue Anwendung, ein Treiber oder eine geänderte Windows-Einstellung –, schalten Sie den Schutz vorübergehend ab:

1. Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
2. Klicken Sie im Menü auf **Schutz deaktivieren** und dann auf **Schutz jetzt deaktivieren**.
3. Bestätigen Sie „Möchten Sie den HDGUARD-Schutz deaktivieren? Der PC wird dazu ohne Nachfrage neu gestartet!“ mit **Ja**. Der PC startet ohne Schutz neu.
4. Nehmen Sie die gewünschten Änderungen vor und installieren Sie ggf. ausstehende Windows-Updates.
5. Aktivieren Sie den Schutz wieder wie unter *Schutz aktivieren* beschrieben.

> **Warnung**
> Änderungen, die Sie **vor** dem Deaktivieren bei aktivem Schutz vornehmen, gehen mit dem Neustart verloren. Installieren Sie Software und Updates erst, nachdem der PC ohne Schutz neu gestartet ist.

> **Tipp**
> Denken Sie daran, den Schutz nach der Wartung wieder zu aktivieren. Das Menü zeigt den Zustand jederzeit an (**Schutz aktiv** / **Schutz inaktiv**).

6.3 Meldungen im Betrieb

Auslastung der Swap-Datei
: Bei aktivem Schutz zeigt das Hauptfenster, wie weit die *Swap-Datei* gefüllt ist (grün bis 50 %, gelb bis 80 %, darüber rot). Sinkt der freie Platz unter 100 MB, warnt HDGUARD: „Warnung! Der freie Platz in der HDGUARD SWAP-Datei beträgt weniger als 100MB. Starten Sie das System bald neu!“ Ein Neustart setzt die Swap-Datei dann zurück.

© 2026 IST Deutschland GmbH

Update-Zeitraum
: Beginnt ein Update-Zeitraum, während Benutzer angemeldet sind, erscheint „Update-Zeitraum 1 beginnt. Das System wird in 30 Sekunden neugestartet!“; der Neustart lässt sich abbrechen. Während des Zeitraums meldet das Hauptfenster „Update-Zeitraum 1 ist aktiv.“

Lizenz
: Läuft eine Frist ab, weist HDGUARD darauf hin, z. B. „Sie haben noch 5 Tag(e), bis Sie die Software-Aktivierung durchführen müssen!“ Siehe *Abgelaufene oder ungültige Lizenz*.

6.4 Darstellung der Oberfläche anpassen

Design, eingeklapptes Menü und das automatische Ausblenden des Anmeldehinweises stellen Sie unter *Info & Einstellungen* ein.

© 2026 IST Deutschland GmbH

Teil III

Weitere Einstellungen und Expertenansicht

© 2026 IST Deutschland GmbH

Kapitel 7

Die Expertenansicht

In diesem Teil wird jeder Bereich der Oberfläche vollständig beschrieben – mit allen Einstellungen, auch denen, die nur in der *Expertenansicht* zugänglich sind. Solche Stellen sind jeweils gekennzeichnet.

7.1 Expertenansicht einschalten

Die Expertenansicht wird über den Schalter **Expertenansicht** am unteren Menürand ein- und ausgeschaltet.

Beim ersten Einschalten erscheint eine Warnung, deren Bestätigung gespeichert wird. Die Warnung erscheint danach nicht mehr für den aktuellen Benutzer. Über **PDF Handbuch öffnen** in der Warnung öffnen Sie dieses Handbuch, ohne die Warnung zu schließen.

Ist der PC mit *HDGUARD.master* verbunden, startet die Oberfläche direkt in der Expertenansicht.

7.2 Was die Expertenansicht zusätzlich bietet

Neue Menüeinträge
: *Sichtbarkeit*, *USB*, *Ausnahmen* und *HDGUARD.master*.

Schutz aktivieren und deaktivieren
: den *Seminar-Modus* mit seinen Rücksetzeinstellungen und die Option *Windows Update weiterhin sperren*.

Festplatten
: alle Partitionen und die *Konfiguration einzelner Partitionen* samt Swap-Datei.

Passwörter
: das *Seminar-Passwort* und die Hinweise zu Admin-Stick und Domänengruppe.

Lizenzierung
: das *Zurücksetzen der Lizenz*.

Update-Zeiträume
: die Zeiträume 2 und 3, weitere Arten und die globalen Benutzereinstellungen (siehe *Update-Zeiträume*).

> ⚠ **Warnung**
> Ändern Sie Einstellungen der Expertenansicht nur, wenn Sie deren Wirkung kennen. Fehlerhafte Festplatten- oder Ausnahme-Einstellungen können Windows unbrauchbar machen oder den Schutz unwirksam werden lassen.

© 2026 IST Deutschland GmbH

Kapitel 8

Schutz aktivieren und deaktivieren

Die erste Aktivierung in der Standardansicht führt *Schutz aktivieren* Schritt für Schritt durch. Dieses Kapitel beschreibt alle Möglichkeiten – einschließlich Seminar-Modus, Multiboot und Windows Update Sperre.

Der Schutz wird immer mit einem Neustart des PCs ein- oder ausgeschaltet. HDGUARD kennt zwei Arten des Schutzes:

Normaler Schutz
: Jeder Neustart setzt den PC auf den Zustand zurück, den er beim Aktivieren des Schutzes hatte.

***Seminar-Modus* (*Expertenansicht*)**
: Änderungen bleiben über Neustarts hinweg erhalten, bis der Seminar-Modus zurückgesetzt wird.

8.1 Schutz aktivieren

Menüeintrag: **Schutz aktivieren** (sichtbar, solange der Schutz ausgeschaltet ist)

8.1.1 Voraussetzungen

- Die *Festplatten-Konfiguration* ist vollständig. Andernfalls zeigt die Ansicht die Warnung „Festplatten-Konfiguration unvollständig“; die Schaltfläche **Festplatten** führt direkt zur Konfiguration.
- Windows wartet nicht auf einen Neustart für Updates. Andernfalls meldet das Hauptfenster „Windows Update benötigt einen Neustart des PCs. Der HDGUARD Schutz kann daher nicht aktiviert werden.“ Starten Sie den PC dann zunächst neu.
- Die Lizenz ist gültig oder der Testzeitraum läuft noch.

8.1.2 Ablauf

1. Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
2. Klicken Sie auf **Schutz jetzt aktivieren**.
3. Bestätigen Sie die Rückfrage „Möchten Sie den HDGUARD-Schutz aktivieren? Der PC wird dazu ohne Nachfrage neu gestartet!“ mit **Ja**.
4. Anschließend wird der PC auf den HDGUARD Schutz vorbereitet und startet neu – mit aktivem Schutz.

Schlägt die Vorbereitung auf den Schutz fehl, zeigt HDGUARD die Fehlermeldung an und nimmt die bereits ausgeführten Schritte automatisch zurück. Das Fenster lässt sich danach nur noch schließen.

Bei aktivem Schutz setzt jeder folgende Neustart den PC wieder auf den Zustand zurück, den er beim Aktivieren hatte.

© 2026 IST Deutschland GmbH

8.2 Multiboot-Systeme

HDGUARD unterstützt Multiboot-Systeme mit dem Windows-Bootmanager.

8.2.1 Multiboot-System einrichten

Für die Einrichtung eines solchen Systems gehen Sie wie folgt vor:

1. Starten Sie das Setup der **höchsten** zu installierenden Windows-Version. Löschen Sie in der Partitionierung alle vorhandenen Partitionen auf der Startfestplatte und legen Sie die Systempartition für diese Windows-Version an. Legen Sie mit diesem Partitionierer auch die Partitionen für die weiteren Windows-Versionen und ggf. eine zusätzliche Partition für ungeschützte Daten an.
2. Brechen Sie das Setup danach ab, statt fortzufahren, und starten Sie das Setup der **ältesten** Windows-Version, die Sie in das Multiboot-System integrieren wollen.
3. Installieren Sie die Windows-Systeme von der ältesten bis zur neuesten Version jeweils in die vorgesehene Partition. Auch Linux®-Systeme können aufgenommen werden; sie müssen ihren Bootcode im Startsektor ihrer jeweiligen Bootpartition ablegen und im Windows-Bootmanager eingetragen werden.

So stellen Sie sicher, dass der aktuelle Windows-Bootmanager verwendet wird und keine Reparatur bestehender Systeme oder externe Werkzeuge nötig sind.

4. Installieren Sie HDGUARD auf jedem Windows-System.
5. Führen Sie die *Festplatten-Konfiguration* auf **einem** Windows-System durch. Jede Partition mit einer Windows-Installation erhält den Modus „Geschützt (Swap-Datei)“, versteckte Startpartitionen „Schreibgeschützt (Read-Only)“ oder „Gesperrt (kein Zugriff)“. Diese Konfiguration gilt für alle Windows-Installationen des Multiboot-Systems; gleiches gilt für die *Software-Aktivierung*.
6. Starten Sie nun – beginnend mit der ältesten Windows-Version – auf jeder Installation die HDGUARD-Oberfläche und aktivieren Sie den Schutz. Auf die Frage „Ist dies die Installation, die automatisch gestartet wird?“ antworten Sie mit **Nein**. Nur bei der Installation, die der Bootmanager automatisch startet – in der Regel die neueste Windows-Version –, antworten Sie mit **Ja**, und zwar zuletzt.

Damit ist sichergestellt, dass alle Windows-Installationen auf den Schutz vorbereitet sind. Für die weiteren Installationen steht auch `HDGcmd /PrepareForProtection` zur Verfügung (siehe *Bedienung per Kommandozeile*).

8.2.2 Rückfrage beim Aktivieren

Erkennt HDGUARD mehrere Einträge im Windows-Bootmenü, erscheint statt der normalen Rückfrage der Dialog **Schutz aktivieren auf Multiboot-System** mit der Frage „Ist dies die Installation, die automatisch gestartet wird?“

Ja
: aktiviert den Schutz.

Nein
: bereitet nur diese Windows-Installation auf den Schutz vor und startet neu, ohne den Schutz einzuschalten.

Abbrechen
: bricht den Vorgang ab.

Beantworten Sie die Frage in der Reihenfolge aus *Schritt 6 der Einrichtung*.

© 2026 IST Deutschland GmbH

8.3 Seminar-Modus

> **Bemerkung**
> Der Seminar-Modus ist nur in der *Expertenansicht* verfügbar.

Im Seminar-Modus führt ein Neustart nicht zum Ausgangszustand zurück. Die Änderungen aus den vorherigen Sitzungen bleiben erhalten, bis

- ein Benutzer den Seminar-Modus zurücksetzt,
- eine konfigurierte *automatische Rücksetzung* fällig wird,
- ein *Update-Zeitraum* beginnt, für den „Im Seminar-Modus Update-Zeitraum erzwingen“ eingeschaltet ist, oder
- der Speicherplatz in der *Swap-Datei* ausgeschöpft ist.

Seminar-Modus einschalten: Schalten Sie in der Ansicht **Schutz aktivieren** den Schalter **Seminar-Modus** ein und aktivieren Sie den Schutz wie oben beschrieben. Der Schalter steht beim Öffnen der Ansicht immer auf „Aus“.

Solange der Seminar-Modus aktiv ist, zeigt der Fenstertitel „HDGUARD, Seminar-Modus aktiv“.

8.3.1 Rücksetzeinstellungen

Die Rücksetzeinstellungen erscheinen in der Ansicht **Schutz aktivieren**, sobald der Seminar-Modus eingeschaltet ist, und in der Ansicht **Schutz deaktivieren**, solange der Seminar-Modus aktiv ist. Änderungen werden sofort übernommen.

Angemeldeter Benutzer darf zurücksetzen
: Der angemeldete Benutzer kann den Seminar-Modus für den nächsten Neustart zurücksetzen – über den Eintrag **System beim Neustart zurücksetzen** im Rechtsklickmenü des Systemtray-Icons (Abb. 8.1). Ist ein *Seminar-Passwort* gesetzt, ist dafür dieses Passwort erforderlich.

Täglich zurücksetzen
: Der Seminar-Modus wird an jedem Tag automatisch zurückgesetzt.

Automatisches Zurücksetzen an diesen Wochentagen / Monatstagen
: Ist „Täglich zurücksetzen“ ausgeschaltet, wählen Sie Wochentage (Mo–So) und / oder Monatstage (1–31). Beide Auswahlen werden mit ODER verknüpft.

> **Bemerkung**
> Ohne gewählte Tage wird der Seminar-Modus nie automatisch zurückgesetzt. HDGUARD prüft bei jedem Start, ob seit dem letzten Zurücksetzen ein gewählter Tag lag; verpasste Tage werden also beim nächsten Start nachgeholt.

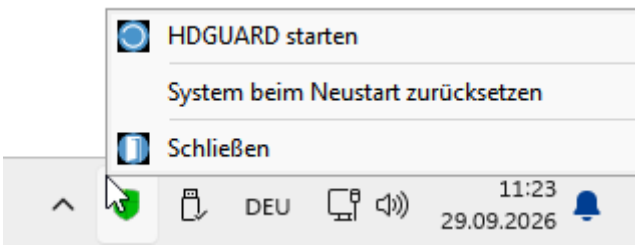


Abb. 8.1: Rechtsklickmenü des Systemtray-Icons

© 2026 IST Deutschland GmbH

8.4 Schutz deaktivieren

Menüeintrag: **Schutz deaktivieren** (sichtbar, solange der Schutz eingeschaltet ist)

1. Speichern Sie alle offenen Dokumente und beenden Sie laufende Anwendungen.
2. Klicken Sie auf **Schutz jetzt deaktivieren**.
3. Bestätigen Sie die Rückfrage „Möchten Sie den HDGUARD-Schutz deaktivieren? Der PC wird dazu ohne Nachfrage neu gestartet!“ mit **Ja**.

Der Schutz endet mit dem Neustart des PCs. Dabei wird der PC auf den ursprünglichen Zustand zurückgesetzt.

> **Warnung**
> Änderungen, die Sie vor dem Deaktivieren bei aktivem Schutz vorgenommen haben, gehen mit diesem Neustart verloren. Installieren Sie Software und Updates erst **nach** dem Deaktivieren.

Der Schutz lässt sich nicht deaktivieren, solange ein Update-Zeitraum für die Software-Verteilung läuft („Der Update-Zeitraum für die Software-Verteilung ist aktiv. Der Schutz kann derzeit nicht deaktiviert werden.“).

8.5 Windows Update und Schutz

Bei aktivem Schutz ist Windows Update abgeschaltet: Updates für Windows und Microsoft Defender lassen sich nur bei deaktiviertem Schutz oder in einem *Update-Zeitraum* installieren. Nach dem Ausschalten des Schutzes schaltet HDGUARD Windows Update standardmäßig wieder ein.

Soll Windows Update auch nach dem Ausschalten des HDGUARD Schutzes gesperrt bleiben – etwa, um zu verhindern, dass nach langem geschütztem Betrieb viele Updates auf einmal nachinstalliert werden –, schalten Sie in der Ansicht **Schutz deaktivieren** die Option **Windows Update weiterhin sperren** ein (*Expertenansicht*). Die Änderung wirkt sofort; das Hauptfenster weist mit „Windows Update wird beim nächsten Neustart ohne HDGUARD-Schutz weiterhin geblockt.“ darauf hin.

Ist Windows Update bei ausgeschaltetem Schutz gesperrt, zeigt die Ansicht **Schutz aktivieren** die Karte **Windows Update Sperre**. Mit **Aufheben** geben Sie Windows Update wieder frei; dies wird mit dem nächsten Neustart wirksam.

> **Tipp**
> Halten Sie das System mit *Update-Zeiträumen* aktuell, statt den Schutz für Updates von Hand zu deaktivieren.

© 2026 IST Deutschland GmbH

Kapitel 9

Festplatten

In der Ansicht **Festplatten** legen Sie fest, welche Partitionen wie geschützt werden. Die automatische Zuweisung bei der ersten Einrichtung beschreibt *Festplatten automatisch zuweisen*; dieses Kapitel beschreibt alle Möglichkeiten, einschließlich der Konfiguration einzelner Partitionen in der *Expertenansicht*.

> **Bemerkung**
> Die Festplatten-Konfiguration lässt sich nur bei ausgeschaltetem Schutz ändern. Bei aktivem Schutz zeigt die Ansicht die Konfiguration nur an („Diese Einstellungen können nicht geändert werden, solange der Schutz aktiv ist.“).

9.1 Darstellung

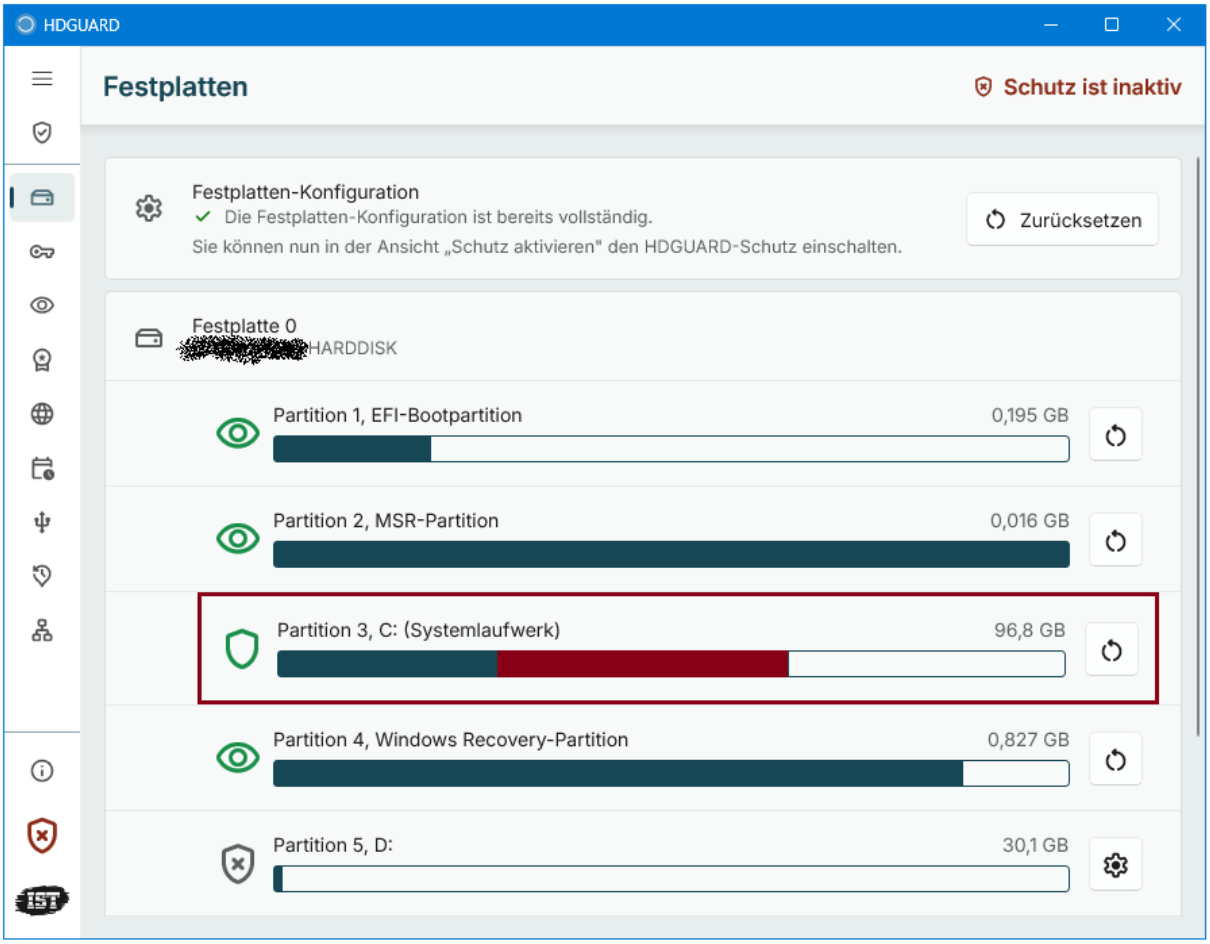


Abb. 9.1: Die Ansicht „Festplatten“ in der Expertenansicht

Für jede Festplatte zeigt die Ansicht eine Karte („Festplatte 0“, „Festplatte 1“ …) mit Hersteller und Modell. Jede Partition erscheint mit Nummer, Laufwerksbuchstabe bzw. Partitionstyp (z. B.

© 2026 IST Deutschland GmbH

„EFI-Bootpartition“, „Windows Recovery-Partition“, „Systemlaufwerk“) und einem Belegungsbalken. Ein Symbol zeigt den Schutzmodus der Partition, der Tooltip des Balkens die Belegung.

Jede mit einer Swap-Datei geschützte Partition hat einen farbigen Rahmen. In derselben Farbe erscheint ihre Swap-Datei als Abschnitt im Belegungsbalken der Partition, auf der die Swap-Datei liegt. So sehen Sie auf einen Blick, wo die Swap-Datei einer geschützten Partition liegt, auch wenn sie auf einer anderen Partition der Festplatte angelegt ist. In Abb. 9.1 liegt die Swap-Datei von `C:` (roter Rahmen) auf `C:` selbst. Der Tooltip des farbigen Abschnitts nennt Größe und – bei aktivem Schutz – Auslastung der Swap-Datei, die geschützte Partition und ggf. das *Swap-RAM*.

Ohne *Expertenansicht* zeigt die Ansicht nur Partitionen mit Laufwerksbuchstaben; EFI-, MSR- und Recovery-Partitionen sind ausgeblendet.

9.2 Schutzmodi je Partition

Schutzmodus	Wirkung
Geschützt (Swap-Datei)	Änderungen werden in eine Swap-Datei umgeleitet und beim Neustart verworfen.
Schreibgeschützt (Read-Only)	Die Partition kann gelesen, aber nicht verändert werden.
Gesperrt (kein Zugriff)	Auf die Partition kann weder lesend noch schreibend zugegriffen werden.
Ungeschützt (kein Schutz)	Die Partition wird von HDGUARD nicht geschützt.
Zielpartition für konfigurierte Ausnahmen	Die Partition dient als *Ausnahmeziel* und kann nicht zugleich geschützt werden (siehe *Ausnahmen*).

Bemerkung
Die Einstellungen werden mit dem Aktivieren des Schutzes wirksam. Eine ungeschützte Partition bleibt auch bei aktivem Schutz beschreibbar; Daten darauf bleiben über Neustarts erhalten.

9.3 Vollständige Konfiguration

Der Schutz lässt sich erst aktivieren, wenn die Konfiguration vollständig ist. Das ist der Fall, wenn

- das Systemlaufwerk `C:` durch eine Swap-Datei geschützt ist und
- alle Start- und Bootpartitionen (EFI, MSR, Recovery sowie eine separate Systempartition) schreibgeschützt sind. MSR- und Recovery-Partitionen dürfen auch gesperrt sein.

Die Karte **Festplatten-Konfiguration** meldet den Zustand: „Die Festplatten-Konfiguration ist bereits vollständig.“ (mit grünem Haken) bzw. „Die Festplatten-Konfiguration ist unvollständig.“ Solange die Konfiguration unvollständig ist, ist die Karte gelb hinterlegt.

9.4 Automatisch zuweisen

Automatisch zuweisen richtet die empfohlene Konfiguration ein:

- Das Systemlaufwerk `C:` erhält eine Swap-Datei auf `C:` selbst. Dafür müssen auf `C:` mehr als 4 GB frei sein.
- Die Größe der Swap-Datei beträgt die Hälfte des freien Speichers, wenn weniger als 64 GB frei sind, sonst 32 GB plus 1/20 des freien Speichers.
- Als *Swap-RAM* wird ca. 1/16 des Arbeitsspeichers reserviert.

© 2026 IST Deutschland GmbH

- Die Start- und Bootpartitionen werden schreibgeschützt.

Lässt sich die automatische Zuweisung nicht durchführen, starten Sie den PC neu und versuchen Sie es erneut. Ist sie grundsätzlich nicht möglich, kontaktieren Sie ggf. den Support.

Zurücksetzen hebt nach einer Rückfrage die gesamte Festplatten-Konfiguration auf.

9.5 Partitionen einzeln konfigurieren

> **Bemerkung**
> Die Konfiguration einzelner Partitionen ist nur in der *Expertenansicht* verfügbar.

Klicken Sie auf das Zahnrad-Symbol einer Partition.

- **Systemlaufwerk:** Für `C:` ist nur der Schutz per Swap-Datei vorgesehen; es öffnet sich direkt der Dialog **Swap-Datei konfigurieren**.
- **Andere Partitionen:** Wählen Sie zunächst den Schutztyp (**Geschützt (Swap-Datei)**, **Schreibgeschützt (Read-Only)** oder **Gesperrt (kein Zugriff)**) und klicken Sie auf **Übernehmen**.

Bei bereits konfigurierten Partitionen erscheint statt des Zahnrads ein Symbol zum Aufheben der Konfiguration, da ein Schutztyp nicht direkt in einen anderen überführt werden kann.

9.5.1 Swap-Datei konfigurieren

Zielpartition für die Swap-Datei
: Partition, auf der die Swap-Datei angelegt wird. Sie muss auf **derselben Festplatte** liegen, mit NTFS formatiert sein und mehr als 4 GB freien Speicher haben. Vorbelegt ist die Partition selbst.

Größe der Swap-Datei
: Speicherplatz, der für die Swap-Datei reserviert wird – mindestens 512 MB. Die Vorbelegung folgt derselben Regel wie *Automatisch zuweisen*.

Swap-RAM reservieren
: Arbeitsspeicher, der reserviert wird, um die ersten Umleitungen in die Swap-Datei zu beschleunigen – bis zu einem Viertel des Arbeitsspeichers. Vorbelegt ist beim Systemlaufwerk 1/16 des Arbeitsspeichers, sonst 0.

> **Tipp**
> Swap-RAM belegt einen Teil des Arbeitsspeichers, nutzen Sie dieses Feature möglichst nur für das Systemlaufwerk `C:`.

> **Warnung**
> Die Swap-Datei nimmt alle Änderungen bis zum nächsten Neustart auf. Wählen Sie sie deshalb ausreichend groß. Bei aktivem Schutz zeigt das Hauptfenster ihre Auslastung an; sinkt der freie Platz unter 100 MB, warnt HDGUARD: „Warnung! Der freie Platz in der HDGUARD SWAP-Datei beträgt weniger als 100MB. Starten Sie das System bald neu!“

© 2026 IST Deutschland GmbH

Kapitel 10

Passwörter

Menüeintrag: **Passwort** (in der *Expertenansicht*: **Passwörter**)

Das erste Setzen des Passworts bei der Einrichtung beschreibt *HDGUARD-Passwort setzen*. Dieses Kapitel beschreibt alle Möglichkeiten, einschließlich Seminar-Passwort, Admin-Stick und Domänengruppe.

Das HDGUARD-Passwort schützt die Oberfläche und damit die gesamte Konfiguration. Ohne gesetztes Passwort kann jeder Benutzer HDGUARD öffnen und den Schutz abschalten. Es könnte auch ein Ihnen unbekanntes Passwort gesetzt werden und so die Installation oder das ganze System unbrauchbar werden. Das Hauptfenster weist dann mit „Diese HDGUARD-Installation ist nicht durch ein HDGUARD-Passwort geschützt.“ darauf hin.

> **⚠ Warnung**
> Achten Sie unbedingt darauf, das Passwort nicht zu verlegen oder zu vergessen. Es gibt keine fest einprogrammierten Passwörter und keine Möglichkeit, ein vergessenes Passwort wiederherzustellen.

10.1 HDGUARD-Passwort setzen, ändern oder entfernen

Die Karte **HDGUARD-Passwort** zeigt, ob ein Passwort gesetzt ist. Solange kein Passwort gesetzt ist, ist die Karte rot hinterlegt.

1. Klicken Sie auf **Setzen** bzw. **Ändern**.
2. Geben Sie beim Ändern zunächst das **Aktuelles HDGUARD-Passwort** ein.
3. Geben Sie das **Neues Passwort** ein und wiederholen Sie es.
4. Bestätigen Sie mit **OK**.

Passwörter dürfen höchstens 16 Zeichen lang sein. Eine Anzeige bewertet die Qualität des neuen Passworts mit „Schwach“, „OK“ oder „Stark“ („Stark“ ab 12 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen). Die Bewertung ist ein Hinweis und verhindert das Setzen nicht. Mit **Passwörter anzeigen** machen Sie die Eingaben sichtbar.

Passwort entfernen: Lassen Sie beim Ändern beide Felder für das neue Passwort leer.

> **ℹ Bemerkung**
> Im Testzeitraum kann kein Passwort gesetzt werden. Ein bereits gesetztes Passwort lässt sich bei ungültiger Lizenz nur noch entfernen.

10.2 Seminar-Passwort

> **ℹ Bemerkung**
> Das Seminar-Passwort ist nur in der *Expertenansicht* sichtbar.

© 2026 IST Deutschland GmbH

Das Seminar-Passwort schützt das Zurücksetzen des *Seminar-Modus* durch Benutzer. Ohne Seminar-Passwort kann bei aktiver Option **Angemeldeter Benutzer darf zurücksetzen** jeder Benutzer den Seminar-Modus zurücksetzen.

Das Seminar-Passwort lässt sich nur setzen, wenn

- die Lizenz gültig ist,
- ein HDGUARD-Passwort gesetzt ist und
- Sie sich mit dem HDGUARD-Passwort angemeldet haben.

10.3 Anmeldung ohne Passworteingabe

10.3.1 Admin-Stick

Ein *Admin-Stick* ist ein angelernter USB-Stick, mit dem sich Lehrkräfte, Servicepersonal oder Aushilfen bei HDGUARD anmelden können, ohne das Passwort zu kennen. Admin-Sticks werden in der Ansicht *USB* angelernt.

Zur Anmeldung stecken Sie den Stick an und wählen im Anmeldedialog **Admin-Stick Anmeldung**. Die Schaltfläche erscheint nur, wenn ein angelernter Admin-Stick angeschlossen ist.

Bei einer Anmeldung über den Admin-Stick

- lassen sich die Passwörter nicht ändern,
- lässt sich die Liste der angelernten USB-Sticks nur ansehen, nicht ändern, exportieren oder importieren.

Wird der Stick während der Sitzung abgezogen, sperrt HDGUARD die Oberfläche („Admin-Stick entfernt – Ohne den Stick sind keine Aktionen mehr möglich.“). Beenden Sie die Oberfläche mit **HDGUARD beenden** und starten Sie sie neu, um sich wieder anzumelden.

10.3.2 Domänengruppe „HDGUARD-Administrators“

Ist der PC Mitglied einer Domäne (Active Directory), können sich Mitglieder der Domänen-Sicherheitsgruppe **HDGUARD-Administrators** ohne Passwort anmelden. Wählen Sie dazu im Anmeldedialog **Domänengruppen Anmeldung**.

- Die Gruppe muss zuvor in der Domäne angelegt und mit Mitgliedern versehen werden. Globale, universelle und domänenlokale Gruppen sind zulässig; verschachtelte Mitgliedschaften werden berücksichtigt.
- Die Ansicht **Passwörter** (*Expertenansicht*) zeigt, ob der angemeldete Benutzer Mitglied der Gruppe ist.
- Wie beim Admin-Stick lassen sich die Passwörter bei dieser Anmeldeart nicht ändern.

© 2026 IST Deutschland GmbH

Kapitel 11

Sichtbarkeiten

Menüeintrag: **Sichtbarkeit**

> **Bemerkung**
> Die Ansicht ist nur in der *Expertenansicht* sichtbar. Die Schalter lassen sich erst mit gültiger Lizenz bedienen, nicht im Testzeitraum.

Vielfach soll die Präsenz von HDGUARD vor den Benutzern verborgen bleiben. In dieser Ansicht legen Sie fest, wo HDGUARD in Erscheinung tritt – von voll sichtbar bis unsichtbar. Änderungen werden sofort übernommen.

11.1 Verknüpfungen

Einträge im Windows Startmenü
: Legt die Einträge von HDGUARD im Startmenü an.

Verknüpfung auf dem Windows Desktop
: Legt ein HDGUARD-Symbol auf dem Desktop an. Ein Doppelklick startet die Oberfläche.

Die Verknüpfungen lassen sich nur bei ausgeschaltetem Schutz ändern.

> **Bemerkung**
> Ohne Einträge im Startmenü oder bei Benachrichtigungsstummschaltung werden HDGUARD-Benachrichtigungen nicht mehr über das Windows-Benachrichtigungssystem angezeigt sondern als einfache Dialogfenster.

11.2 Benutzeroberfläche

Hinweisfenster beim Einloggen anzeigen
: Zeigt beim Einloggen ein Produktfenster an, das den Benutzer über den Schutz des PCs informiert.

Systemtray-Icon anzeigen
: Zeigt ein HDGUARD-Symbol im Infobereich der Taskleiste. Es ist ratsam, dieses Symbol immer anzuzeigen.

Statusfenster bei Maus-Hover über Systemtray-Icon anzeigen
: Zeigt beim Daraufzeigen mit dem Mauszeiger ein Fenster mit Schutzstatus und Versionsinformation.

Rechtsklickmenü des Systemtray-Icons aktivieren
: Bietet schnellen Zugriff auf HDGUARD-Aktionen über einen Rechtsklick auf das Symbol.

Lokale- und Domänenadministratoren bei den Sichtbarkeitseinschränkungen ignorieren
: Administratorkonten sehen HDGUARD immer vollständig.

Statusfenster und Rechtsklickmenü lassen sich nur einschalten, wenn das Systemtray-Icon angezeigt wird.

© 2026 IST Deutschland GmbH

Tipp
Windows versteckt das HDGUARD-Symbol im Infobereich der Taskleiste. Nutzen Sie ggf. Gruppenrichtlinien, um die Symbole für alle Benutzer sichtbar zu schalten.

© 2026 IST Deutschland GmbH

Kapitel 12

Lizenzierung

Menüeintrag: **Lizenzierung** (immer verfügbar)

In dieser Ansicht geben Sie den Lizenzschlüssel ein, führen die Software-Aktivierung durch und sehen die Lizenzinformationen ein. Die Grundlagen zu Testzeitraum, Lizenzschlüssel und Software-Aktivierung beschreibt *Lizenzierung und Testzeitraum*, den kürzesten Weg bei der ersten Einrichtung *Lizenzschlüssel eingeben und Software aktivieren*.

Die Karte **Lizenz** zeigt oben die *Gerätekennung* dieses PCs („Die Gerätekennung für die Software-Aktivierung ist: …“), darunter die *Lizenzinformationen* und die Schaltflächen:

Setzen bzw. Ändern
: öffnet die Eingabe des Lizenzschlüssels. Solange kein Lizenzschlüssel eingegeben ist, heißt die Schaltfläche **Setzen**; die Zeile mit den Schaltflächen ist dann gelb hinterlegt und zeigt den Hinweis „Kein Lizenzschlüssel eingegeben.“

Software-Aktivierung
: führt die Software-Aktivierung über das Internet durch. Nur sichtbar, wenn ein Lizenzschlüssel eingegeben ist.

Zurücksetzen
: setzt Lizenzierung und Software-Aktivierung dieses PCs zurück. Nur in der *Expertenansicht* und bei eingegebenem Lizenzschlüssel sichtbar.

12.1 Lizenzschlüssel eingeben

1. Klicken Sie auf **Setzen** (ist bereits ein Schlüssel eingegeben: **Ändern**).
2. Geben Sie im Dialog **Lizenzschlüssel eingeben** den 20-stelligen Schlüssel ein. Großschreibung und Bindestriche (`XXXXX-XXXXX-XXXXX-XXXXX`) ergänzt HDGUARD selbst.
3. Sobald der Schlüssel vollständig ist, prüft HDGUARD ihn online und zeigt die höchste lizenzierte HDGUARD-Version und die Anzahl der Clients an.
4. Bestätigen Sie mit **OK**.
5. Führen Sie anschließend die Software-Aktivierung durch.

Ist die Online-Prüfung nicht möglich, wird der Schlüssel trotzdem übernommen. Meldet der Server dagegen, dass die installierte Version höher als die lizenzierte ist oder die Lizenz keine Clients enthält, kann der Schlüssel nicht übernommen werden.

12.2 Software-Aktivierung über das Internet

Klicken Sie auf **Software-Aktivierung**. Die Aktivierung startet sofort und wird mit „Die Software-Aktivierung über das Internet wurde erfolgreich durchgeführt.“ bestätigt.

© 2026 IST Deutschland GmbH

12.3 Offline Software-Aktivierung

Kann der PC keine Verbindung zum Aktivierungsserver aufbauen, öffnet sich der Dialog **Offline Software-Aktivierung**:

1. Klicken Sie auf **Aktivierungsdatei exportieren** und speichern Sie die Datei. Vorgeschlagen wird der Name `HDGUARD-<PC-Name>-Request.haf` (wie bei `/RequestFileActivation`); so bleibt erkennbar, von welchem PC die Anfrage stammt. Nach dem Export öffnet sich ein Explorer Fenster mit dem Pfad der Datei.
2. Kopieren Sie die Datei auf einen PC mit Internetverbindung und laden Sie sie auf der Webseite https://license-de.ist.com hoch.
3. Die Webseite erzeugt eine PC-spezifische Aktivierungsdatei. Kopieren Sie diese zurück auf den zu aktivierenden PC.
4. Rufen Sie die Software-Aktivierung erneut auf und wählen Sie im Dialog **Aktivierungsdatei importieren**.

Die Offline-Aktivierung ist auch per *Kommandozeile* möglich (`/RequestFileActivation`, `/SetActivationAnswer`).

12.4 Lizenz zurücksetzen

Zurücksetzen (*Expertenansicht*) meldet die Software-Aktivierung dieses PCs beim Lizenzserver ab und entfernt den Lizenzschlüssel. Verwenden Sie diese Funktion, wenn der PC ausgemustert oder die Lizenz auf einem anderen PC eingesetzt werden soll.

12.5 Lizenz wechseln

Geben Sie einen anderen Lizenzschlüssel ein, gibt HDGUARD die bisherige Aktivierung beim Lizenzserver automatisch frei. Anschließend ist eine neue Software-Aktivierung erforderlich. Gleiches gilt, wenn sich die Gerätekennung des PCs geändert hat.

12.6 Lizenzinformationen

Angabe	Bedeutung
Lizenzsignatur	die ersten fünf Zeichen des Lizenzschlüssels
Ungültig ab	Monat/Jahr, ab dem die Lizenz nicht mehr gilt
Höchste HDGUARD Version	höchste Hauptversion, die mit dieser Lizenz betrieben werden darf
HDGUARD Clients	Anzahl unterschiedlicher PCs, auf denen HDGUARD installiert werden darf
HDGUARD.master mitlizenziert	ob die Lizenz *HDGUARD.master* enthält; falls ja, zusätzlich die Module HDGUARD.remote, HDGUARD.deploy und HDGUARD.os sowie die maximale Anzahl der HDGUARD.master Clients
INiS mitlizenziert	ob die Lizenz INiS enthält; falls ja, zusätzlich Version und Anzahl der Clients

Eine Kurzfassung (Signatur, Gültigkeit, Lizenzgröße) finden Sie auch unter *Info & Einstellungen*.

© 2026 IST Deutschland GmbH

Bemerkung
Wenn der Lizenzserver https://license-de.ist.com erreichbar ist, versucht HDGUARD regelmäßig, seine Lizenzinformationen zu aktualisieren. Wenn die Subskriptionsperiode also demnächst verlängert wird, werden dadurch automatisch auch die „Ungültig ab“ Informationen aktualisiert.

© 2026 IST Deutschland GmbH

Kapitel 13

Internet-Einstellungen

Menüeintrag: **Internet-Einstellungen** (immer verfügbar, auch ohne Lizenz)

HDGUARD benötigt eine Internetverbindung für die *Software-Aktivierung* und für Windows-Updates in *Update-Zeiträumen*. Führt der Weg ins Internet über einen Proxyserver, müssen Sie ihn hier hinterlegen.

> **Bemerkung**
> Die Einstellungen lassen sich nur bei ausgeschaltetem Schutz ändern.

13.1 Verbindungsart

Direkte Internetverbindung
: Der PC erreicht das Internet ohne Proxyserver.

Internetverbindung über Proxyserver
: Geben Sie die **Proxy-Adresse** und den **Port** ein, bei Bedarf auch **Benutzername (optional)** und **Passwort (optional)**.

Weicht der in Windows konfigurierte Proxy (Gruppenrichtlinie, WinHTTP-Standard oder WPAD) von der Eingabe ab, bietet die Ansicht ihn zur Übernahme an („Aus Systemkonfiguration: …“, **Übernehmen**). Übernommen werden Adresse und Port.

Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen; **Verwerfen** stellt den gespeicherten Stand wieder her.

> **Bemerkung**
> Bei der Software-Aktivierung versucht HDGUARD zunächst eine direkte Verbindung, dann den hier hinterlegten Proxy und zuletzt den Proxy der Windows-Systemkonfiguration.

Den Proxy können Sie auch per *Kommandozeile* (`/SetWebProxy`, `/ShowWebProxy`) oder über *HDGUARD.master* setzen.

© 2026 IST Deutschland GmbH

Kapitel 14

Update-Zeiträume

Menüeintrag: **Update-Zeitraum** (in der *Expertenansicht*: **Update-Zeiträume**; verfügbar mit gültiger Lizenz oder im Testzeitraum)

Damit Betriebssystem und Virenscanner trotz Schutz aktuell bleiben, können Sie Update-Zeiträume einrichten. Während eines Update-Zeitraums startet der PC ohne HDGUARD-Schutz und arbeitet je nach Einstellung automatisierte Aufgaben ab. Dabei ist sichergestellt, dass keine unautorisierte Benutzeranmeldung stattfinden kann.

Einen einfachen Update-Zeitraum für Windows-Updates bei der ersten Einrichtung beschreibt *Update-Zeitraum einrichten (optional)*. Dieses Kapitel beschreibt alle Möglichkeiten, einschließlich der weiteren Zeiträume und Arten in der *Expertenansicht*.

14.1 Zeiträume

Ohne Expertenansicht steht **ein** Update-Zeitraum für Windows-Updates zur Verfügung. In der Expertenansicht können Sie **drei** unabhängige Zeiträume einrichten (**Zeitraum 1** bis **Zeitraum 3**). Jeder Zeitraum wird mit seinem Schalter ein- oder ausgeschaltet und mit **Speichern** übernommen.

> ⚠ **Warnung**
> Speichern Sie ohne Expertenansicht, werden Zeitraum 2 und 3 sowie die globalen Benutzereinstellungen gelöscht.

14.1.1 Einstellungen je Zeitraum

Art des Update-Zeitraums

Windows Update durchführen – sucht und installiert Windows-Updates.

Software-Verteilung durchführen (*Expertenansicht*) – führt Aufträge der Software-Verteilung aus. Erfordert eine Lizenz mit HDGUARD.deploy.

Manuelle Arbeiten durchführen (*Expertenansicht*) – startet den PC ohne Schutz für eigene Arbeiten, optional mit automatischer Anmeldung und einer auszuführenden Befehlszeile.

Dauer (Minuten) bzw. Minimum-Dauer (Minuten)

3 bis 255 Minuten. Bei **Windows Update durchführen** heißt das Feld „Minimum-Dauer“: Werden Windows-Updates geladen und installiert, verlängert HDGUARD die Dauer automatisch. Darauf weist auch das i-Symbol neben der Beschriftung hin.

Startzeit

Uhrzeit, zu der der Update-Zeitraum beginnt.

Täglich ausführen

Der Update-Zeitraum gilt an jedem Tag. Ist die Option ausgeschaltet, wählen Sie **Wochentage** und/oder **Monatstage**. Beide Auswahlen werden mit ODER verknüpft – der Zeitraum gilt an jedem Tag, der auf eine der beiden Auswahlen passt.

Im Seminar-Modus Update-Zeitraum erzwingen (*Expertenansicht*)

Der Update-Zeitraum findet auch im *Seminar-Modus* statt und setzt ihn zu Beginn zurück. Ohne diese Option wird der Zeitraum im Seminar-Modus ignoriert.

© 2026 IST Deutschland GmbH

Am Ende des Zeitraums:
Neustarten oder **Herunterfahren**.

Nur bei „Manuelle Arbeiten durchführen“:

Kommandozeile ausführen
Startet eine lokale, ausführbare Datei (mit vollständigem Pfad).

Automatische Anmeldung / Anmeldung des Admin-Benutzers
Erlaubt die automatische Anmeldung des Auto-Login Benutzers bzw. die Anmeldung des Admin-Benutzers (siehe *Globale Einstellungen*).

14.1.2 Globale Einstellungen

> **Bemerkung**
> Die globalen Einstellungen sind nur in der *Expertenansicht* sichtbar.

(Admin) Benutzer
Benutzer, der sich während eines Update-Zeitraums anmelden darf. Alle anderen Anmeldungen werden abgewiesen.

Auto-Login Benutzer
Benutzername, Domäne und Passwort für die automatische Anmeldung. Während der Benutzer angemeldet ist, sind Bildschirm und Tastatur gesperrt. Ist zusätzlich „Kommandozeile ausführen“ eingeschaltet, wird die Befehlszeile in der Sitzung dieses Benutzers gestartet, sonst in der Sitzung des Dienstes.

14.2 Ablauf eines Update-Zeitraums

- Wird ein Update-Zeitraum im laufenden Betrieb fällig, erhalten angemeldete Benutzer den Hinweis „Update-Zeitraum 1 beginnt. Das System wird in 30 Sekunden neugestartet!“ und können den Neustart abbrechen.
- Während des Zeitraums zeigt der Anmeldebildschirm „Update-Zeitraum 1 wird 60 Minuten ausgeführt.“ Nicht zugelassene Benutzer werden abgemeldet.
- Das Hauptfenster meldet „Update-Zeitraum 1 ist aktiv.“
- Dauert die Installation von Windows-Updates länger als der Zeitraum, verlängert sich der Zeitraum automatisch, bis die Installation abgeschlossen ist.
- Verlangt ein Update einen Neustart, startet HDGUARD den PC neu und setzt den Update-Zeitraum danach fort.
- Am Ende startet der PC neu bzw. fährt herunter, sobald kein Benutzer mehr angemeldet ist – anschließend wieder mit aktivem Schutz.

> **Warnung**
> Neustarts innerhalb eines Update-Zeitraums erfolgen ohne Nachfrage. Sind Sie als zugelassener Benutzer angemeldet, beendet ein solcher Neustart Ihre Sitzung!

Für Windows-Updates verwendet HDGUARD den unter *Internet-Einstellungen* hinterlegten Proxy.

Jeden Schritt – vom Beginn des Zeitraums über Suche, Download und Installation der Windows-Updates bis zum Neustart – protokolliert HDGUARD im *Ereignisprotokoll*.

© 2026 IST Deutschland GmbH

14.3 Spezielle Update-Zeiträume

Neben den konfigurierten Update-Zeiträumen startet HDGUARD in folgenden Situationen selbstständig einen kurzen, automatischen Update-Zeitraum:

Zeitumstellung
: HDGUARD erkennt die automatische Umstellung zwischen Sommer- und Winterzeit. Der erste Start danach erfolgt ohne Schutz und ohne Möglichkeit der Benutzeranmeldung; nach etwa zwei Minuten startet der PC automatisch mit aktivem Schutz neu.

Software-Verteilung
: Wird über *HDGUARD.master* Software auf diesen PC verteilt, so wird ein automatischer Update-Zeitraum für die Verteilung durchlaufen. Dies geschieht auch, wenn der HDGUARD-Schutz gar nicht eingeschaltet ist.

Bootschleifen
: Um Bootschleifen durch Windows-Updates mit integriertem Neustart zu verhindern, startet nach mehr als fünf Neustarts ohne Benutzeranmeldung in Folge ein automatischer Update-Zeitraum. Auch er endet nach etwa zwei Minuten.

Angemeldete Benutzer erhalten dabei den Hinweis „Automatischer Update-Zeitraum! Ein Neustart folgt in Kürze!“ und werden abgemeldet.

© 2026 IST Deutschland GmbH

Kapitel 15

USB-Sticks

Menüeintrag: **USB**

> **Bemerkung**
> Die Ansicht ist nur in der *Expertenansicht* sichtbar (mit gültiger Lizenz oder im Testzeitraum).

HDGUARD kann die Nutzung von USB-Massenspeichern einschränken und einzelne USB-Sticks trotzdem zulassen. Angelernte Sticks mit Admin-Eigenschaft dienen zusätzlich zur Anmeldung bei HDGUARD.

15.1 Behandlung der lokalen USB-Massenspeicher

USB uneingeschränkt zulassen
: USB-Massenspeicher können ohne Einschränkung genutzt werden.

Schreiben sperren (nur Lesen erlaubt)
: USB-Massenspeicher können gelesen, aber nicht beschrieben werden.

Lesen und Schreiben sperren
: USB-Massenspeicher können nicht genutzt werden.

15.2 Zugelassene USB-Massenspeicher

Geräte in der Liste werden trotz der globalen Sperre als Massenspeicher zugelassen. Die Liste zeigt je Gerät, ob es ein *Admin-Stick* ist, die Bezeichnung und die Gerätekennung des Sticks.

15.2.1 Stick anlernen

1. Geben Sie unter **Neuen Stick anlernen** eine Bezeichnung ein (erforderlich, höchstens 31 Zeichen).
2. Klicken Sie auf **Stick anlernen** bzw. **Admin-Stick anlernen**.
3. Stecken Sie den Stick innerhalb von 15 Sekunden an und klicken Sie auf **Erledigt**.

Ein *Admin-Stick* ermöglicht zusätzlich die Anmeldung bei HDGUARD ohne Passwort und darf den Schutz deaktivieren (siehe *Passwörter*).

Mit **Ausgewählten Stick entfernen** und **Alle entfernen** löschen Sie Einträge; **Aktualisieren** lädt die Liste neu.

15.2.2 Liste übertragen

Mit **Liste exportieren...** und **Liste importieren...** übertragen Sie die Regeln für USB-Sticks auf andere PCs (Datei `USBlist.bin`). Der Import fügt die Einträge an die lokale Liste an.

Per *Kommandozeile* stehen dafür `/ExportUSBsticks` und `/ImportUSBsticks` zur Verfügung.

© 2026 IST Deutschland GmbH

Bemerkung
Bei einer Anmeldung über einen Admin-Stick lässt sich die Liste nur ansehen. Anlernen, Entfernen, Export und Import erfordern das HDGUARD-Passwort; die Behandlung der USB-Massenspeicher können Sie weiterhin umstellen.

© 2026 IST Deutschland GmbH

Kapitel 16

Ausnahmen

Menüeintrag: **Ausnahmen**

> **Bemerkung**
> Die Ansicht ist nur in der *Expertenansicht* sichtbar (mit gültiger Lizenz oder im Testzeitraum). Änderungen sind nur bei ausgeschaltetem Schutz möglich.

HDGUARD schützt Festplatten immer **per Partition**. Einzelne Dateien oder Ordner innerhalb einer geschützten Partition lassen sich grundsätzlich nicht vom Schutz ausnehmen. Gleiches gilt für die Windows-Registrierung, die in mehreren Dateien auf dem Systemlaufwerk `C:` abgelegt ist.

Für eng begrenzte Fälle bietet HDGUARD zwei Techniken an:

- **Verzeichnisverbindungen:** Ein Ordner auf `C:` wird per Verzeichnisverbindung auf die Ausnahmepartition umgeleitet. Er liegt scheinbar auf `C:`, das Dateisystem leitet den Zugriff aber auf einen versteckten Ordner der Ausnahmepartition um. Dateien darin bleiben nach einem Neustart erhalten.
- **Registry-Ausnahmen:** Die Inhalte der gewählten Registry-Schlüssel werden regelmäßig auf der Ausnahmepartition gesichert und beim Hochfahren frühzeitig wiederhergestellt, sodass Änderungen erhalten bleiben.

Beide benötigen eine ungeschützte Partition, das *Ausnahmeziel*.

> **Warnung**
> Ausnahmen schwächen den Schutz gezielt ab: Alles, was in einer Ausnahme liegt, übersteht den Neustart – auch unerwünschte Änderungen. Richten Sie Ausnahmen nur ein, wenn es keine andere Lösung gibt, etwa *Update-Zeiträume*.

16.1 Ausnahmeziel festlegen

Als Ausnahmeziel eignet sich eine Partition, die

- auf derselben Festplatte wie `C:` liegt (kein USB-Datenträger),
- einen eigenen Laufwerksbuchstaben hat,
- nicht von HDGUARD geschützt wird und
- mindestens 1 GB freien Speicher hat.

Wählen Sie unter **Ausnahmeziel festlegen** die Partition aus und klicken Sie auf **Diese Partition verwenden**. Die Ansicht *Festplatten* kennzeichnet sie danach als „Zielpartition für konfigurierte Ausnahmen“.

© 2026 IST Deutschland GmbH

16.1.1 Ausnahmepartition anlegen

Gibt es keine geeignete Partition, legt **Neue Partition auf der Boot-Festplatte anlegen…** direkt hinter `C:` eine neue an:

1. Geben Sie die **Größe der neuen Partition (GB)** an – mindestens 1,5 GB, damit nach der Formatierung mindestens 1 GB frei bleibt. Vorhandener freier Speicher hinter `C:` wird mitgenutzt; reicht er nicht, wird `C:` verkleinert.
2. Legen Sie **Datenträger-Bezeichnung** und **Laufwerksbuchstabe** fest.
3. Klicken Sie auf **Partition erstellen**.
4. Starten Sie den PC anschließend neu, damit HDGUARD die neue Partition erkennt.

> **Warnung**
> Schalten Sie den PC während des Vorgangs nicht aus und starten Sie ihn nicht neu.

Alternativ können Sie die Partition mit der Windows-Datenträgerverwaltung anlegen; nach einem Neustart erscheint sie in der Auswahl.

16.1.2 Ausnahmen zurücksetzen

Ausnahmen zurücksetzen entfernt die Markierung der Ausnahmepartition und alle eingetragenen Registry-Ausnahmen und Verzeichnisverbindungen.

16.2 Registry-Ausnahmen

1. Klicken Sie unter **Registry-Ausnahmen** auf **Hinzufügen…**.
2. Wählen Sie einen Schlüssel unter `HKLM\SOFTWARE` oder `HKLM\SYSTEM` aus oder geben Sie den Pfad ein. Mit einem Schloss gekennzeichnete Bereiche lassen sich nicht weiter aufklappen, sind aber auswählbar.
3. Bestätigen Sie mit **Hinzufügen**.

> **Bemerkung**
> Schlüssel, die für den Start des Betriebssystems von Bedeutung sind, lassen sich nicht sinnvoll ausnehmen, da die Sicherung erst während des Starts zurückgespielt wird. Ebenso wenig Schlüssel, die beim Start noch nicht geladen sind, etwa aus dem Zweig des angemeldeten Benutzers (`HKCU`).

16.3 Verzeichnisverbindungen auf C:

1. Klicken Sie unter **Verzeichnisverbindungen auf C:** auf **Hinzufügen…**.
2. Wählen Sie mit **Durchsuchen…** den übergeordneten Ordner auf `C:`.
3. Geben Sie den Namen der Verzeichnisverbindung ein. Der Ordner darf noch nicht existieren. **Resultierender Pfad:** zeigt den vollständigen Pfad.
4. Bestätigen Sie mit **Hinzufügen**.

Ausgewählte auflösen bzw. **Alle auflösen** hebt Verzeichnisverbindungen wieder auf; der Inhalt wird dabei nach `C:` verschoben.

© 2026 IST Deutschland GmbH

Kapitel 17

HDGUARD.master

Um HDGUARD-Clients mit dem optionalen Programm *HDGUARD.master* verwalten zu können, baut jeder Client eine TCP/IP-Verbindung zu dem PC oder Server auf, auf dem der zentrale HDGUARD.master-Dienst installiert ist.

17.1 Verbindung einrichten

Menüeintrag: **HDGUARD.master**

> **Bemerkung**
> Die Ansicht ist nur in der *Expertenansicht* sichtbar (mit gültiger Lizenz oder im Testzeitraum). Änderungen sind nur bei ausgeschaltetem Schutz möglich.

Die Statuskarte zeigt, ob eine Verbindung besteht („Verbindung zu HDGUARD.master aufgebaut“), über welche Verbindungsart und zu welchem Server. Ist HDGUARD.deploy lizenziert, zeigt eine weitere Karte den Status der Software-Verteilung.

Unter **Verbindungsart** wählen Sie:

LAN
: Direkte Verbindung im lokalen Netzwerk. Achten Sie darauf, dass die angegebene Adresse auflösbar und erreichbar ist.

NAT
: Verbindung über Netzwerkadressübersetzung. Erfordert eine spezielle Einrichtung am Server.

HDGUARD.remote Online-Server
: Verbindung über den Online-Server von IST, sodass sich PCs auch außerhalb des lokalen Netzes verwalten lassen. Erfordert eine spezielle Einrichtung und Lizenzierung von HDGUARD.master (Modul HDGUARD.remote) sowie einen eingegebenen Lizenzschlüssel.

Bei LAN und NAT geben Sie **Server** (Name oder IP-Adresse) und **Server-Port** ein. Ohne abweichende Einstellung gelten:

- Server: `HDGUARDmaster`
- Port: `52234`

> **Warnung**
> Ändern Sie den Port nur, wenn Sie vom Support dazu aufgefordert werden.

Mit **Anwenden und speichern** wird die Verbindung sofort neu aufgebaut; das kann bis zu 30 Sekunden dauern.

> **Tipp**
> In größeren Netzwerken empfiehlt es sich, im DNS-Server einen Alias (CNAME) `HDGUARDmaster` für den Server mit dem zentralen HDGUARD.master-Dienst einzutragen. Dann funktionieren die Standardwerte ohne weitere Einstellung.

© 2026 IST Deutschland GmbH

Die Verbindungsdaten lassen sich auch bei der Installation per *MSI-Parameter* übergeben.

17.1.1 Einstellungen in der Registry

Die Verbindungsdaten liegen unter `HKEY_LOCAL_MACHINE\SOFTWARE\IST\HDGUARD`:

Wert	Typ	Bedeutung
`Server`	REG_SZ	Name oder IP-Adresse des HDGUARD.master-Servers
`ServerPort`	REG_DWORD	Port (Standard 52234)
`AltConn`	REG_DWORD	Verbindungsart: 0 = LAN, 1 = NAT, 2 = HDGUARD.remote
`RemoteServer`, `RemoteServerPort`	REG_SZ / REG_DWORD	Online-Server für HDGUARD.remote

Von Hand geänderte Werte werden beim nächsten Start des PCs eingelesen. Deaktivieren Sie vor einem solchen Eingriff den Schutz.

> **Bemerkung**
> Die Ablage der Werte hat sich für den Remote-Fall gegenüber HDGUARD-Version 12 geändert.

17.2 Benachrichtigungen für angemeldete Benutzer

Einige Aktionen von HDGUARD.master kann HDGUARD dem angemeldeten Benutzer ankündigen – als Windows-Benachrichtigung mit Countdown oder als Meldungsfenster:

Bildschirmschnappschuss
: Fordert der Administrator einen Screenshot an, muss der Benutzer dies zulassen: „Erlauben Sie dem Administrator, in dieser Sitzung Bildschirmschnappschüsse zu erstellen?“ Er hat dafür 30 Sekunden Zeit. Lehnt er ab, erhält HDGUARD.master ein Platzhalterbild.

Abmelden
: „Sie werden innerhalb von 30 Sekunden abgemeldet!“ Der Benutzer kann die Abmeldung mit **Abbrechen** verhindern.

Herunterfahren / Neustart
: „Ausstehendes Herunterfahren des Systems!“ bzw. „Ausstehender Neustart des Systems!“ – ebenfalls mit 30 Sekunden Zeit zum Abbrechen.

© 2026 IST Deutschland GmbH

Kapitel 18

Info und Einstellungen

Menüeintrag: **Info & Einstellungen** (am unteren Menürand)

Einstellungen und Info erscheinen in einem Dialog. **PDF Handbuch öffnen** öffnet dieses Handbuch in Ihrem PDF-Programm und schließt den Dialog.

18.1 Einstellungen

Menü beim Start minimiert darstellen
: Das Menü wird auch bei großem Fenster eingeklappt dargestellt. Wirkt ab dem nächsten Start.

Anwendung in folgendem Design darstellen
: **Anpassen an Windows**, **Helles Design** oder **Dunkles Design**. Wirkt sofort.

Anmeldehinweis automatisch ausblenden
: Blendet die Hinweise zur Art der Anmeldung („Authentifiziert über …“) nach fünf Sekunden automatisch aus.

Telemetrie-Daten senden
: Erlaubt das Erfassen, Übermitteln und Auswerten der Konfiguration, um das Produkt weiter zu verbessern. Standardmäßig ausgeschaltet.

Die ersten drei Einstellungen gelten je Windows-Benutzer, die Telemetrie gilt für den ganzen PC.

18.1.1 Telemetrie

Mit eingeschalteter Telemetrie überträgt HDGUARD

- den aktuellen HDGUARD-Zustand,
- alle Optionen, die Sie in der HDGUARD-Oberfläche einstellen können,
- die Windows-Systemumgebung und
- relevante Hardwareinformationen (CPU, Arbeitsspeicher, Festplatten, Bildschirmauflösung).

Zeichenketten wie Pfade, Namen oder Ähnliches werden nicht erhoben. Die Daten werden nur bei der Software-Aktivierung und -Deaktivierung an den Lizenzserver übertragen.

Die Telemetrie lässt sich bei der Installation auch per *MSI-Parameter* `TELEMETRY` festlegen.

Wird die Software-Aktivierung mit dem *HDGUARD.master* durchgeführt, entscheidet der Master, ob die Telemetriedaten gesendet werden (siehe *HDGUARD.master*).

18.2 Info

Der Info-Bereich zeigt

- die Lizenz (Signatur, Gültigkeit und Lizenzgröße, siehe *Lizenzierung*) und
- die installierte HDGUARD-Version.

© 2026 IST Deutschland GmbH

Teil IV

Automatisierung und Referenz

© 2026 IST Deutschland GmbH

Kapitel 19

Bedienung per Kommandozeile

Um HDGUARD automatisiert per Skript oder aus einer Eingabeaufforderung zu steuern, starten Sie `HDGcmd.exe` aus dem Programmverzeichnis (`C:\Program Files\IST\HDGUARD`) mit den entsprechenden Parametern. Ein Aufruf ohne oder mit unkorrekten Parametern zeigt die Kommandozeilenhilfe in Englisch an.

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

Numerische Ergebnisse gibt `HDGcmd` über die Umgebungsvariable `ERRORLEVEL` zurück. Negative Werte bezeichnen einen Fehler, 0 bedeutet in der Regel Erfolg.

19.1 Verschlüsselte Passwörter

Befehle, die ein Passwort erfordern, erwarten es **verschlüsselt** (Platzhalter `PWD`). Die verschlüsselte Form erzeugt `/EncryptPWD`. Auch das leere Passwort (solange keines gesetzt ist) muss verschlüsselt übergeben werden:

```
> HDGcmd /EncryptPWD ""
ndwevu7Msgu4/IZgOrznSOETN7vh9iRU8djZ+oQjs/shMH/M4+gkN4jCJ+R6VasS

> HDGcmd /EncryptPWD "MyS3cr3tPassw0rd"
hEb8CLS8S4saLdJgzt3QCC51sRja+DTpd4mwxqb/PBfQdWDGdcAH4Qe8+PKdcd7+
```

19.2 Befehle

19.2.1 Passwörter

Befehl	Wirkung
`/EncryptPWD "password"`	Verschlüsselt das angegebene Passwort für die `PWD`-Platzhalter.
`/SetPassword PWD newPWD`	Setzt das HDGUARD-Passwort.
`/SetUserPassword PWD newUPWD`	Setzt das *Seminar-Passwort*.
`/SetMasterPassword MPWD newMPWD`	Setzt das *Service-Passwort*.

19.2.2 Schutz

Befehl	Wirkung
`/GetMode`	Gibt den aktuellen Schutzmodus zurück (Werte siehe unten).
`/GetModeInConfig`	Gibt den für den nächsten Neustart geplanten Schutzmodus zurück.
`/ActivateProtection PWD`	Aktiviert den normalen Schutz und startet neu.
`/ActivateSeminarMode PWD`	Aktiviert den Seminar-Modus und startet neu.
`/DeactivateProtection PWD`	Deaktiviert den Schutz und startet neu.
`/PrepareForProtection PWD`	Bereitet diese Windows-Installation auf den Schutz vor und startet neu. Nur für die weiteren Installationen eines *Multiboot-Systems*!
`/SetSeminarReset PWD 1`	Der nächste Neustart setzt den Seminar-Modus zurück.
`/SetSeminarReset PWD 0`	Der nächste Neustart setzt den Seminar-Modus nicht zurück.
`/GetSeminarReset`	Gibt den mit `/SetSeminarReset` gesetzten Wert zurück.

Rückgabewerte von `/GetMode` und `/GetModeInConfig`:

Wert	Schutzmodus
0	Schutz deaktiviert
1	Schutz aktiv
2	Seminar-Modus aktiv
4	automatischer Update-Zeitraum (*Spezielle Update-Zeiträume*)
5	Update-Zeitraum für Windows-Updates
6	Update-Zeitraum für die Software-Verteilung
7	Update-Zeitraum 1
8	Update-Zeitraum 2
9	Update-Zeitraum 3

Bemerkung
Die englische Kommandozeilenhilfe nennt für die Update-Zeiträume 1 bis 3 die Werte 6 bis 8. Maßgeblich ist die Tabelle oben.

© 2026 IST Deutschland GmbH

19.2.3 Festplatten

Befehl	Wirkung
`/ListPartitions`	Zeigt Informationen zu allen Partitionen, darunter den Index `i`, mit dem die folgenden Befehle eine Partition ansprechen.
`/AutoConfig PWD`	Versucht eine *automatische Konfiguration* der Partitionen.
`/ResetVolume PWD i`	Hebt den Schutzmodus der Partition `i` auf.
`/SetVolumeProtected PWD i t s r`	Schützt die Partition `i` mit einer Swap-Datei auf Partition `t` (meist `t = i`), Größe `s` MB (üblich 16384) und Swap-RAM `r` MB (üblich 32 für `C:`, sonst 0).
`/SetVolumeReadOnly PWD i`	Setzt die Partition `i` auf „Schreibgeschützt“.
`/SetVolumeNoAccess PWD i`	Setzt die Partition `i` auf „Gesperrt“.
`/GetUsage i`	Gibt die Auslastung der Swap-Datei der Partition `i` in Prozent zurück.

`/ListPartitions` gibt je Partition den HDGUARD-Index, Festplatte und Partitionsnummer, Laufwerk, Größe und freien Speicher, den Schutzmodus und – bei geschützten Partitionen – Größe und Ort der Swap-Datei sowie das konfigurierte und das genutzte Swap-RAM aus. USB-Datenträger werden nicht aufgeführt.

Beispiel bei ausgeschaltetem Schutz:

```
> HDGcmd /ListPartitions
-------------------------------------------------------------------------------
HDGUARD index 1, LastIndex: FALSE
Hard drive 0, partition 1: \\?\Volume{fce5d809-1b13-4ae2-9e27-c4d364275a78}\
Size: 200 MB, free space: 161 MB
-------------------------------------------------------------------------------
HDGUARD index 2, LastIndex: FALSE
Hard drive 0, partition 2:
Size: 16 MB
-------------------------------------------------------------------------------
HDGUARD index 3, LastIndex: FALSE
Hard drive 0, partition 3: C:\
Size: 109941 MB, free space: 86612 MB
-------------------------------------------------------------------------------
HDGUARD index 4, LastIndex: FALSE
Hard drive 0, partition 4: D:\
Size: 19999 MB, free space: 19944 MB
-------------------------------------------------------------------------------
HDGUARD index 5, LastIndex: TRUE
Hard drive 0, partition 5: \\?\Volume{dcbdcd17-1ec0-445d-8217-f02d6a7c0468}\
Size: 912 MB, free space: 115 MB
```

© 2026 IST Deutschland GmbH

Derselbe PC bei aktivem Schutz: `C:` ist mit einer Swap-Datei geschützt, EFI-, MSR- und Recovery-Partition sind schreibgeschützt, `D:` ist ungeschützt.

```
> HDGcmd /ListPartitions
-------------------------------------------------------------------------------
HDGUARD index 1, LastIndex: FALSE
Hard drive 0, partition 1: \\?\Volume{fce5d809-1b13-4ae2-9e27-c4d364275a78}\
Size: 200 MB, free space: 161 MB
HDGUARD mode: 1 (READ_ONLY)
-------------------------------------------------------------------------------
HDGUARD index 2, LastIndex: FALSE
Hard drive 0, partition 2:
Size: 16 MB
HDGUARD mode: 1 (READ_ONLY)
-------------------------------------------------------------------------------
HDGUARD index 3, LastIndex: FALSE
Hard drive 0, partition 3: C:\
Size: 109941 MB, free space: 49521 MB
HDGUARD mode: 2 (REDIRECTED),
SWAP-File: 37098 MB on index 3, SWAP-Ram set: 512 MB, SWAP-Ram used: 512 MB
-------------------------------------------------------------------------------
HDGUARD index 4, LastIndex: FALSE
Hard drive 0, partition 4: D:\
Size: 19999 MB, free space: 19944 MB
-------------------------------------------------------------------------------
HDGUARD index 5, LastIndex: TRUE
Hard drive 0, partition 5: \\?\Volume{dcbdcd17-1ec0-445d-8217-f02d6a7c0468}\
Size: 912 MB, free space: 119 MB
HDGUARD mode: 1 (READ_ONLY)
```

Die Angaben im Einzelnen:

Angabe	Bedeutung
`HDGUARD index`	Index `i`, mit dem die Befehle oben die Partition ansprechen.
`LastIndex`	`TRUE` beim letzten Eintrag der Liste.
`Hard drive`, `partition`	Festplatten- und Partitionsnummer, dahinter der Laufwerksbuchstabe oder – ohne Laufwerksbuchstaben – der Volume-Pfad. Partitionen ohne Dateisystem (z. B. MSR) haben keinen Namen.
`Size`, `free space`	Größe und freier Speicher in MB. Der freie Speicher fehlt, wenn Windows ihn nicht ermitteln kann.
`HDGUARD mode`	Schutzmodus: `1` schreibgeschützt, `2` mit Swap-Datei geschützt, `3` gesperrt. Fehlt die Zeile, ist die Partition derzeit nicht geschützt – bei ausgeschaltetem Schutz gilt das für alle Partitionen.
`SWAP-File`, `on index`	Größe der *Swap-Datei* und Index der Partition, auf der sie liegt.
`SWAP-Ram set`, `SWAP-Ram used`	Konfiguriertes und derzeit genutztes *Swap-RAM*.
`This volume is marked as target …`	Die Partition ist das *Ausnahmeziel*.

© 2026 IST Deutschland GmbH

19.2.4 Lizenzierung

Befehl	Wirkung
`/SetLicense PWD XXXXXXXXXXXXXXXXXXX`	Setzt den Lizenzschlüssel – ohne Leerzeichen und Bindestriche.
`/DoOnlineActivation`	Führt die Software-Aktivierung über das Internet durch.
`/RequestFileActivation "FULL_PATH_TO_FOLDER"`	Speichert eine Aktivierungsdatei für die *Offline-Aktivierung* im angegebenen Ordner.
`/SetActivationAnswer "FULL_PATH_TO_FILE"`	Importiert die Antwortdatei der Offline-Aktivierung.

19.2.5 Sichtbarkeit

Befehl	Wirkung
`/SetVisibility PWD b b b b`	Vier Werte (0 oder 1) für Hinweisfenster beim Einloggen, Systemtray-Icon, Statusfenster und Rechtsklickmenü des Systemtray-Icons.
`/SetStartmenuLink b`	Schaltet die Startmenü-Einträge ein (1) oder aus (0).
`/SetDesktopLink b`	Schaltet die Desktop-Verknüpfung ein (1) oder aus (0).

19.2.6 Internet und Windows Update

Befehl	Wirkung
`/SetWebProxy PWD [ProxyNameOrIP Port ["ProxyLoginName" "ProxyPassword"]]`	Setzt den Proxy für Internetverbindungen. Ohne weitere Angaben wird der Proxy entfernt.
`/ShowWebProxy PWD`	Zeigt die Proxy-Einstellungen an.
`/DoWindowsUpdates PWD`	Sucht sofort nach Windows-Updates und installiert sie. Bei aktivem Schutz startet der PC dazu in einen besonderen Update-Zeitraum.
`/DisableWUAUperm PWD`	Windows Update bleibt nach dem Deaktivieren des Schutzes gesperrt.
`/EnableWUAUperm PWD`	Windows Update wird nach dem Deaktivieren des Schutzes wieder eingeschaltet.

19.2.7 USB-Sticks

Befehl	Wirkung
`/ExportUSBsticks PWD`	Exportiert die Liste der zugelassenen USB-Sticks nach `C:\ProgramData\IST\USBlist.bin`.
`/ImportUSBsticks PWD`	Importiert die Liste aus `C:\ProgramData\IST\USBlist.bin`.

© 2026 IST Deutschland GmbH

19.2.8 Ausnahmeliste für den Benutzermodus-Schutz

Befehl	Wirkung
`/ShowUMPexclude PWD`	Zeigt die Ausnahmeliste des Benutzermodus-Schutzes (UMP).
`/AddUMPexclude PWD "exe"`	Fügt ein lokales Programm (vollständiger Pfad zur `.exe`) hinzu. Die Datei muss existieren.
`/DelUMPexclude PWD "exe"`	Entfernt ein Programm aus der Liste.

Bemerkung
Nur wenn Sie vom Support dazu aufgefordert werden, ändern Sie diese Liste.

© 2026 IST Deutschland GmbH

Kapitel 20

Klonen

HDGUARD lässt sich in ein Master-Image aufnehmen und mit diesem auf viele PCs verteilen. Beim Klonen wird die Festplatten-Konfiguration im Allgemeinen zurückgesetzt; HDGUARD erkennt den ersten Start nach dem Klonen und richtet die Festplatten dann automatisch ein.

20.1 Installation in einen Klon-Master

1. Richten Sie das Betriebssystem und alle Anwendungen ein.
2. Installieren Sie HDGUARD (siehe *Installation*).
3. Führen Sie die Konfiguration in der HDGUARD-Oberfläche durch. **Richten Sie dabei noch keine Festplatten-Partitionen ein.**
4. Legen Sie bei Bedarf die Registry-Werte für die *automatische Einrichtung* an.
5. Fertigen Sie von diesem Zustand das Image an.

> ⚠ **Warnung**
> HDGUARD darf nicht mit bereits konfigurierten Festplatten geklont werden!

Die Software-Aktivierung muss nach dem Klonen auf jedem Klon erfolgen, da sie an die *Gerätekennung* des jeweiligen PCs gebunden ist. Für die weitere Einrichtung der Klone stehen die *Kommandozeile* und ggf. *HDGUARD.master* zur Verfügung.

20.2 Automatische Einrichtung nach dem Klonen

Der erste Start nach dem Klonen wird in der Regel erkannt, und HDGUARD führt eine automatische Festplatten-Konfiguration durch:

- Das Systemlaufwerk `C:` wird in jedem Fall automatisch konfiguriert (siehe *Automatisch zuweisen*).
- Die von Windows angelegten Startpartitionen werden schreibgeschützt.
- Ist vor dem Klonen ein Lizenzschlüssel eingegeben worden, versucht HDGUARD anschließend die Software-Aktivierung über das Internet.

Den erkannten ersten Start vermerkt HDGUARD im *Ereignisprotokoll* (Ereignis-ID 288).

Die Einrichtung lässt sich mit Registry-Werten unter `HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig` steuern, die Sie vor dem Erstellen des Images anlegen:

`HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\RedirVolumes`
: Legen Sie für jede Partition, die geschützt werden soll, einen DWORD- oder QWORD-Wert an. Name des Werts ist das Laufwerk (z. B. `D:`), der Wert die Größe der Swap-Datei in MB. Für `C:` ist ein Eintrag nur nötig, wenn die Swap-Datei eine von der Automatik abweichende Größe erhalten soll.

© 2026 IST Deutschland GmbH

`HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig\EncPasswords`
: Ist ein HDGUARD-Passwort gesetzt, hinterlegen Sie es hier als Zeichenfolge (REG_SZ) mit dem Namen `PWD` – verschlüsselt mit `HDGcmd /EncryptPWD` (siehe *Bedienung per Kommandozeile*).

Nach der automatischen Konfiguration löscht HDGUARD den gesamten Zweig `HKLM\SOFTWARE\IST\HDGUARD\AutoReConfig`.

> **Bemerkung**
> Die Internet-Proxy Einstellungen bleiben über das Klonen hinaus erhalten.

© 2026 IST Deutschland GmbH

Kapitel 21

Unbeaufsichtigte Installation (MSI-Parameter)

Das HDGUARD-Setup `HDGUARD13_64.msi` bzw. `HDGUARD13_ARM64.msi` lässt sich mit `msiexec` unbeaufsichtigt installieren. Folgende Parameter werden angeboten:

Parameter	Bedeutung
`HDGMASTERNAME`	Name oder IP-Adresse des Systems mit dem zentralen HDGUARD.master-Dienst (Standard `HDGUARDmaster`)
`HDGMASTERPORT`	vom Standard (52234) abweichender Port des HDGUARD.master-Dienstes
`HDGALTCONN`	Verbindungsart zu HDGUARD.master: `0` = LAN, `1` = NAT, `2` = HDGUARD.remote
`HDGREMOTESERVERNAME`	Online-Server für HDGUARD.remote (Standard `hdgremote.ist.com`)
`HDGREMOTESERVERPORT`	Port des Online-Servers (Standard 52234)
`INSTALL_TEACHER`	`INSTALL_TEACHER=yes` installiert die *Lehrerkonsole* mit (kleingeschrieben).
`HDGLICENSE`	Lizenzschlüssel, 20 Zeichen ohne Bindestriche
`HDGPASSWORD`	HDGUARD-Passwort
`TELEMETRY`	*Telemetrie*: `Y` oder `J` = ein, `N` = aus

Hinweise:

- Ohne Angabe bleiben bei einem Update die vorhandenen Werte erhalten, bei einer Neuinstallation gelten die Standardwerte.
- Mit `HDGLICENSE` versucht HDGUARD nach der Installation die Software-Aktivierung über das Internet.
- `HDGPASSWORD` wird nur übernommen, wenn eine gültige Lizenz vorliegt und noch kein Passwort gesetzt ist.

> **⚠ Warnung**
> Achten Sie bei den Parametern, insbesondere beim Passwort, darauf, dass die Kommandozeile bestimmte Zeichen als Steuer- und Trennzeichen behandelt und nicht unverändert an das Setup übergibt.

Beispiel für eine unbeaufsichtigte Installation:

```
msiexec /i HDGUARD13_64.msi /qn HDGMASTERNAME=MyHDGUARDmasterPC INSTALL_
↪TEACHER=yes TELEMETRY=Y
```

© 2026 IST Deutschland GmbH

Auch bei der unbeaufsichtigten Installation startet der PC am Ende neu.

© 2026 IST Deutschland GmbH

Kapitel 22

Lehrerkonsole

Die HDGUARD-Lehrerkonsole stellt bestimmte Funktionen von *HDGUARD.master* an einem Dozentenplatz innerhalb eines HDGUARD.master-Raumes zur Verfügung. Sie können damit HDGUARD-Clients aufwecken und herunterfahren sowie den Bildschirm, die Tonausgabe, das Internet oder die Drucker sperren und freigeben.

Die Lehrerkonsole funktioniert nur zusammen mit HDGUARD.master. Installieren Sie sie nur an den Arbeitsplätzen, an denen auch Dozenten arbeiten – im Setup über die Option „HDGUARD Lehrerkonsole installieren“ oder per *MSI-Parameter* `INSTALL_TEACHER=yes`.

Die Bedienung beschreibt das Handbuch zu HDGUARD.master.

© 2026 IST Deutschland GmbH

Kapitel 23

Ereignisprotokoll

HDGUARD protokolliert wichtige Vorgänge im Windows-Ereignisprotokoll **Anwendung**. Sie finden die Einträge in der Ereignisanzeige unter **Windows-Protokolle › Anwendung**; mit **Aktuelles Protokoll filtern …** grenzen Sie sie nach Ereignisquelle und Ereignis-ID ein.

Zwei Dienste schreiben Einträge:

Ereignisquelle `HDGUARD Service`
: Der HDGUARD-Dienst (`HDhks.exe`) protokolliert Update-Zeiträume, die Installation von Windows-Updates, den ersten Start nach dem Klonen und die Einrichtung der Software-Verteilung. Die Meldungen erscheinen in der Sprache von Windows (Deutsch oder Englisch).

Ereignisquelle `RDTserv`
: Der Dienst RDTserv, über den HDGUARD unter anderem die Eingabe in den Benutzersitzungen sperrt, protokolliert seinen Start, Startfehler und sein Beenden – immer mit der Ereignis-ID 1 und englischem Text.

Werte mit vorangestelltem `0x` sind hexadezimale Fehlercodes von Windows bzw. von Windows Update (z. B. `0×80240022`).

> **Bemerkung**
> Beide Ereignisquellen richten sich beim ersten Start ihres Dienstes selbst ein. Die Texte der Meldungen von `HDGUARD Service` stehen in `HDhks.exe` – nach der Deinstallation kann die Ereignisanzeige ältere Einträge deshalb nur noch ohne Beschreibung anzeigen.

23.1 HDGUARD Service

23.1.1 Update-Zeiträume

Aufgabenkategorie „Ereignisse zu Update-Zeiträumen“:

© 2026 IST Deutschland GmbH

ID	Art	Meldung	Wann
289	Information	Update-Zeitraum *n* startet	Der PC ist in einen geplanten *Update-Zeitraum* (1 bis 3) gestartet.
290	Information	Benutzerdefinierter Prozess erfolgreich gestartet	Bei „Manuelle Arbeiten durchführen“ wurde die eingetragene Kommandozeile gestartet.
291	Fehler	Benutzerdefinierter Prozess konnte nicht gestartet werden 0x*Code*	Die eingetragene Kommandozeile ließ sich nicht starten (z. B. `0×2`: Datei nicht gefunden).
292	Information	Kurzer Update-Zeitraum automatisch gestartet	Ein *automatischer Update-Zeitraum* hat begonnen (nach einer Zeitumstellung oder wiederholten Neustarts ohne Anmeldung), oder Windows-Updates wurden per *Kommandozeile* (`/DoWindowsUpdates`) bzw. über HDGUARD.master angestoßen.
293	Warnung	Benutzer *Name* meldet sich in Sitzung *n* an und wird zwangsweise abgemeldet.	Während eines Update-Zeitraums hat sich ein nicht zugelassener Benutzer angemeldet; HDGUARD meldet ihn ab. In automatischen Update-Zeiträumen gilt das für jeden Benutzer.
294	Information	Lokale Uhr erfolgreich abgeglichen	Zu Beginn jedes Update-Zeitraums gleicht HDGUARD die Uhr des PCs mit dem Zeitserver ab.
295	Fehler	Konnte die lokale Uhr nicht abgleichen 0x*Code*	Der Zeitabgleich ist fehlgeschlagen, z. B. weil kein Zeitserver erreichbar ist.

23.1.2 Windows-Updates

Aufgabenkategorie „Ereignisse zu Windows Update“. Während eines Update-Zeitraums der Art „Windows Update durchführen“ protokolliert der Dienst jeden Schritt – hier in der Reihenfolge des Ablaufs:

© 2026 IST Deutschland GmbH

ID	Art	Meldung	Bedeutung
262	Information	Keine Windows-Updates verfügbar	Die Suche hat keine Updates gefunden.
263	Information	*n* Windows-Update(s) verfügbar	Anzahl der gefundenen Updates.
269	Warnung	Das folgende Windows-Update benötigt während der Installation Benutzereingaben. Es wird ausgelassen! *Titel*	Solche Updates installiert HDGUARD nicht automatisch. Installieren Sie sie bei deaktiviertem Schutz.
296	Warnung	Der Download des folgenden Windows-Updates ist größer als 2 GB. Es wird ausgelassen! *Titel*	Wie oben, z. B. bei Funktionsupdates.
270	Information	Windows-Update Nr. *n* wird heruntergeladen: *Titel*	Je Update, das heruntergeladen wird.
271	Information	Es gibt kein Windows-Update zum Herunterladen	Alle gefundenen Updates wurden ausgelassen.
277	Information	*n* Windows-Update(s) erfolgreich heruntergeladen	Der Download ist abgeschlossen.
286	Information	Die Installation der Windows-Updates beginnt	
298	Information	Update *n* wurde erfolgreich abgeschlossen.	Ergebnis je Update.
299	Fehler	Update *n* wurde mit Fehler 0x*Code* installiert.	Das Update ist installiert, Windows Update meldet aber einen Fehler.
300	Fehler	Update *n* wurde nicht installiert. Fehler 0x*Code*.	
301	Fehler	Update *n* wurde abgebrochen. Fehler 0x*Code*.	
283	Warnung	Ein Neustart wird angesetzt!	Mindestens ein Update verlangt einen Neustart. HDGUARD startet den PC neu und setzt den Update-Zeitraum danach fort.
284	Information	Kein Neustart notwendig	

Die folgenden Fehler bedeuten, dass ein Schritt der Windows-Update-Schnittstelle fehlgeschlagen ist; der Update-Lauf endet dann ohne Installation. Häufigste Ursache ist eine fehlende Internetverbindung oder ein falsch eingetragener Proxy – prüfen Sie die *Internet-Einstellungen*.

© 2026 IST Deutschland GmbH

ID	Meldung
256	CoCreateInstance CLSID_UpdateSession fehlgeschlagen 0x*Code*
257	CoCreateInstance CLSID_UpdateCollection fehlgeschlagen 0x*Code*
258	Konnte UpdateSearcher nicht erstellen 0x*Code*
259	Konnte nicht nach Windows-Updates suchen 0x*Code*
260	Konnte die UpdateCollection nicht abrufen 0x*Code*
261	Konnte die Größe der UpdateCollection nicht ermitteln 0x*Code*
264	Konnte UpdateDownloader nicht erstellen 0x*Code*
265	Konnte Eintrag *n* nicht abrufen 0x*Code*
266	Konnte den Titel von Eintrag *n* nicht ermitteln 0x*Code*
267	Konnte das Installationsverhalten des Windows-Updates nicht ermitteln: *Titel* – Fehlercode 0x*Code*
268	Konnte nicht ermitteln, ob das Windows-Update Benutzereingaben benötigt: *Titel* – Fehlercode 0x*Code*
272	Konnte die UpdateCollection nicht sichern 0x*Code*
273	Downloadfehler 0x*Code*
274	Konnte den UpdateInstaller nicht erstellen 0x*Code*
275	Konnte die Windows-Updates nicht vom UpdateDownloader abrufen 0x*Code*
276	Konnte die Anzahl der heruntergeladenen Windows-Updates nicht ermitteln 0x*Code*
278	Konnte heruntergeladenes Update *n* nicht abrufen 0x*Code*
279	Fehler 0x*Code* beim Akzeptieren der EULA des Windows-Updates: *Titel*
280	Konnte die Windows-Updates nicht für die Installation bereitstellen 0x*Code*
281	Fehler beim Installieren der Windows-Updates 0x*Code*
282	Konnte die Neustartinformation nicht erhalten 0x*Code*
285	Konnte keinen WebProxy erstellen 0x*Code*

23.1.3 Allgemeine Ereignisse

Aufgabenkategorie „Allgemeine Dienstereignisse“:

ID	Art	Meldung	Wann
288	Information	Erster Start nach dem Klonen erkannt. Die automatische Einrichtung wird gestartet.	HDGUARD hat den ersten Start eines Klons erkannt und richtet die Festplatten automatisch ein (siehe *Automatische Einrichtung nach dem Klonen*).
297	Fehler	Fehler beim Erstellen des IST_SWD_USER. HRESULT 0x*Code*	Beim Einrichten der Software-Verteilung durch HDGUARD.master ließ sich das Benutzerkonto für die Verteilung nicht anlegen.

© 2026 IST Deutschland GmbH

23.2 RDTserv

Alle Einträge haben die Ereignis-ID 1:

Art	Meldung	Bedeutung
Information	RDTserv started in normal Mode	Der Dienst ist regulär gestartet.
Information	RDTserv started in compatibility Mode	Der Dienst ist gestartet, bindet seine Komponenten aber nicht in die laufenden Programme ein (Kompatibilitätsmodus). Davor steht ggf. einer der drei folgenden Fehler.
Fehler	LoadInjectionDriver failed	Der Hilfstreiber für die Einbindung ließ sich nicht laden.
Fehler	InjectLibrary RDTclient64.dll failed	Die 64-Bit-Komponente ließ sich nicht einbinden.
Fehler	InjectLibrary RDTclient32.dll failed	Die 32-Bit-Komponente ließ sich nicht einbinden.
Fehler	Could not load preferences	Der Dienst konnte seine Einstellungen nicht laden und beendet sich.
Fehler	Could not create IPC queue	Die interne Kommunikation mit dem HDGUARD-Dienst ließ sich nicht einrichten; der Dienst beendet sich.
Information	Shut down	Der Dienst wurde beendet.

© 2026 IST Deutschland GmbH

Kapitel 24

Glossar

Admin-Stick
: In HDGUARD angelernter USB-Stick, mit dem sich Personen ohne Kenntnis des Passworts bei HDGUARD anmelden können. Er darf den Schutz deaktivieren, aber keine Passwörter ändern.

Ausnahmeziel
: Ungeschützte Partition auf der Boot-Festplatte, auf der Registry-Ausnahmen gesichert und Verzeichnisverbindungen abgelegt werden. Auch Ausnahmepartition genannt.

Expertenansicht
: Ansicht der HDGUARD-Oberfläche, die zusätzliche Bereiche und Einstellungen einblendet. Wird am unteren Menürand ein- und ausgeschaltet.

Gerätekennung
: Die Gerätekennung wird aus dem TPM-Chip des PCs gebildet. An sie ist die Software-Aktivierung gebunden.

HDGUARD.master
: Optionales Programm zur zentralen Steuerung und Überwachung der HDGUARD-geschützten PCs im Netzwerk.

Neustart
: Neustart von Windows. Bei aktivem Schutz verwirft HDGUARD dabei alle Änderungen auf den geschützten Partitionen.

Partition
: Logisch abgegrenzter Bereich einer Festplatte, unter Windows meist mit einem Laufwerksbuchstaben (z. B. `C:`) erreichbar.

Registry-Ausnahme
: Registry-Schlüssel unter `HKLM\SOFTWARE` oder `HKLM\SYSTEM`, dessen Inhalt über Neustarts hinweg erhalten bleibt.

Seminar-Modus
: Art des Schutzes, bei der Änderungen über Neustarts hinweg erhalten bleiben, bis der Seminar-Modus zurückgesetzt wird.

Service-Passwort
: Das Service-Passwort ist eine zusätzliche Autorisierungsschicht, wenn beispielsweise zentrale Verwaltungen vorinstallierte HDGUARD-PCs verteilen. Lokale Administratoren können ihre eigenen HDGUARD-Passwörter setzen und die Zentrale hat weiterhin mit ihrem Service-Passwort Zugriff auf diese PCs.

Software-Aktivierung
: Registrierung einer HDGUARD-Installation beim Hersteller. Sie ist neben dem Lizenzschlüssel für den dauerhaften Betrieb erforderlich.

Swap-Datei
: Datei, in die HDGUARD die Änderungen an einer geschützten Partition umleitet. Ihr Inhalt wird beim Neustart verworfen.

© 2026 IST Deutschland GmbH

Swap-RAM
: Reservierter Arbeitsspeicher, der die ersten Umleitungen in die Swap-Datei beschleunigt.

Update-Zeitraum
: Geplantes Zeitfenster, in dem der PC ohne Schutz startet, um z. B. Windows-Updates dauerhaft zu installieren.

Verzeichnisverbindung
: Ordner auf `C:`, dessen Inhalt auf das Ausnahmeziel umgeleitet wird und daher Neustarts übersteht.

© 2026 IST Deutschland GmbH

Stichwortverzeichnis

A

Admin-Stick, 29, 30, **64**
Anmeldung, 11
Ausnahmen, 42
Ausnahmeziel, 42, **64**
AutoReConfig, 54

B

Betrieb, 18

D

Design, 46
Domänengruppe, 29, 30

E

Einrichtung
    erste, 14
Einstellungen, 46
Ereignisanzeige, 59
Ereignisprotokoll, 59
Erster Start, 14
Expertenansicht, 21, **64**

F

Fernverwaltung, 44
Festplatten, 26

G

Gerätekennung, 8, **64**

H

HDGcmd, 48
HDGUARD.master, 44, **64**
HDGUARD.remote, 44
HDGUARD-Administrators, 30

I

Internet-Einstellungen, 36

K

Klonen, 54
Kommandozeile, 48

L

Lehrerkonsole, 58
Lizenz, 8
    eingeben, 33

M

MSI-Parameter, 56
Multiboot-System, 23

N

Neustart, **64**

P

Partition, 26, **64**
Passwort, 29
Proxy, 36

R

Registry-Ausnahme, 42, **64**

S

Schutz
    aktivieren, 22
    deaktivieren, 25
    Funktionsprinzip, 2
Seminar-Modus, 24, **64**
Service-Passwort, **64**
Sichtbarkeit, 31
Software-Aktivierung, 8, **64**
    durchführen, 33
    offline, 34
Sperre, 11
Splashscreen, 31
Statusanzeige, 12
Swap-Datei, 26, **64**
Swap-RAM, 28, **65**
Systemtray-Icon, 31

T

Telemetrie, 46, 56
Testzeitraum, 8

U

unbeaufsichtigte Installation, 56
Update-Zeitraum, 37, **65**
USB-Massenspeicher, 40
USB-Sticks, 40

V

Verzeichnisverbindung, 42, **65**

W

Wartung, 18
Windows Update, 25, 37

© 2026 IST Deutschland GmbH