O&O software

O&O ShutUp10++

Inhaltsverzeichnis

1 Einführung 2

2 Erste Schritte 3

2.1 Funktionsvergleich 4

2.2 Free Edition 5

2.3 Premium Edition 6

2.4 Erste Schritte 7

3 Funktionen 8

3.1 KI-Entfernung 9

3.2 Profile & Export 10

3.3 Profildateistruktur 11

3.4 Bearbeitungsmodus 12

3.5 Einstellungsdialog 13

4 Premium-Funktionen 14

4.1 Automatischer Schutz 15

4.2 Profil-Editor 16

4.3 Premium-Übersicht 17

5 Datenschutzeinstellungen 18

5.1 Überblick 19

5.2 Telemetriesteuerung 20

5.3 Standortdienste 21

5.4 Windows Update 22

5.5 Cortana & Suche 23

5.6 App-Berechtigungen 24

5.7 Windows Explorer 25

5.8 Sicherheitseinstellungen 26

6 FAQ 27

O&O ShutUp10 Dokumentation

Willkommen zur offiziellen Dokumentation von **O&O ShutUp10** — dem kostenlosen und Premium-Antispionagetool für Windows 10 und Windows 11 von O&O Software GmbH.

Was ist O&O ShutUp10?

O&O ShutUp10 gibt Ihnen die volle Kontrolle über die Datenschutzeinstellungen in Windows 10 und Windows 11. Sie entscheiden, welche unerwünschten Funktionen deaktiviert werden sollen, um Ihre persönlichen Daten privat zu halten. Das Tool verwaltet eine Vielzahl von Windows-Datenschutz- und Telemetrieeinstellungen in einer einzigen, benutzerfreundlichen Oberfläche — ohne tiefgreifende Registry-Kenntnisse.

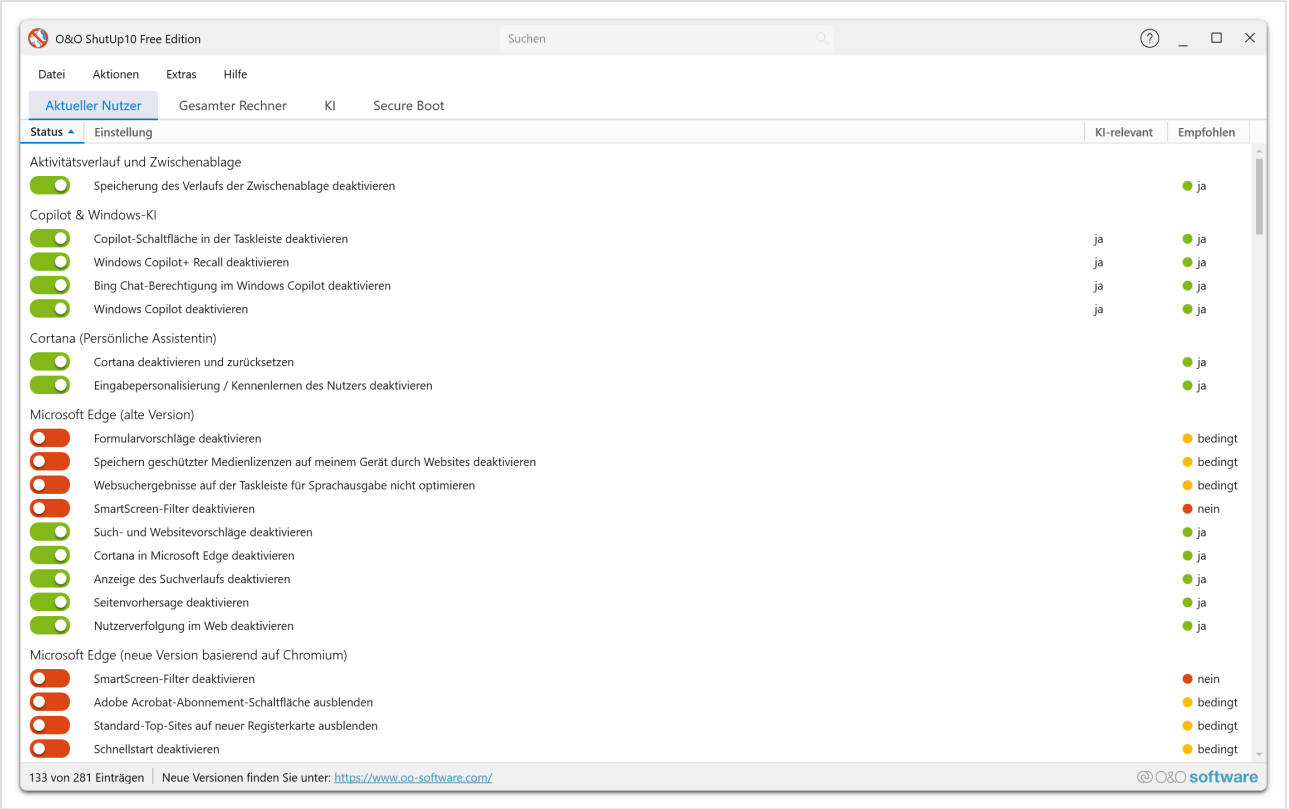
Wichtige Vorteile

- **Volle Datenschutzkontrolle** — Verwalten Sie fast 300 datenschutzrelevante Einstellungen in Windows 10 und Windows 11.
- **Keine Installation erforderlich (Free Edition)** — Direkt als portable Anwendung ausführbar.
- **Klare Empfehlungen** — Jede Einstellung enthält eine Empfehlungsstufe, damit Sie wissen, was sicher zu ändern ist.
- **Änderungen jederzeit rückgängig machen** — Alle Änderungen können mit einem einzigen Klick rückgängig gemacht werden.
- **Völlig kostenlos (Free Edition)** — Die Free Edition ist und bleibt kostenlos.

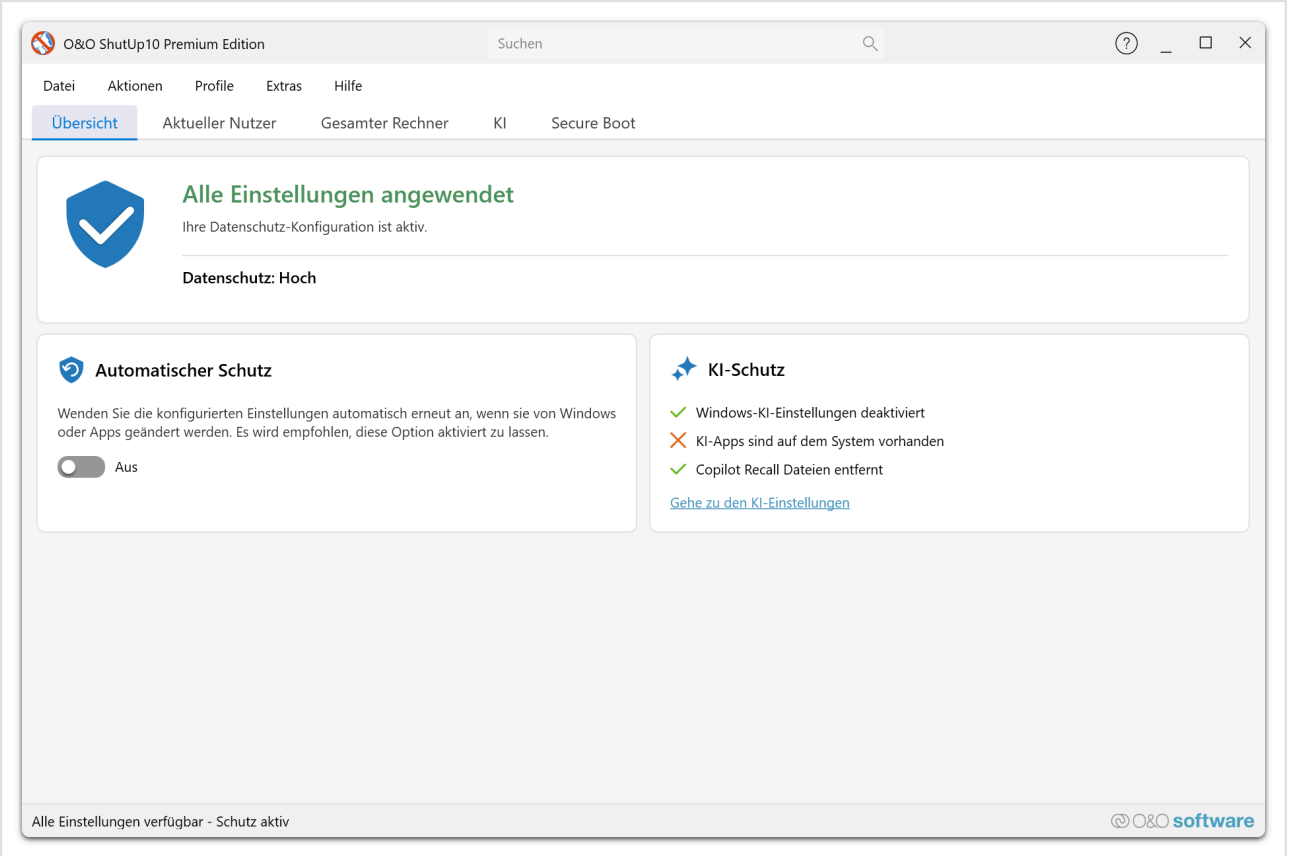
Editionen im Überblick

O&O ShutUp10 ist in zwei Editionen erhältlich, die jeweils für unterschiedliche Einsatzzwecke und Umgebungen konzipiert sind.

Free Edition



Premium Edition



Free Edition

Die **Free Edition** ist ein portables Standalone-Tool, das keine Installation erfordert. Es ist eine leistungsstarke Wahl für Einzelbenutzer, die sofortige, vollständige Kontrolle über ihre Windows-Datenschutzeinstellungen möchten — mit fast 300 Einstellungen, klaren Empfehlungen und ohne Kosten.

- Portabel — läuft direkt von der ausführbaren Datei, kein Setup erforderlich.
- Volle Abdeckung der Datenschutzeinstellungen — die gleichen ca. 300 Einstellungen wie die Premium Edition.
- Jede Datenschutzänderung wird interaktiv vom Benutzer vorgenommen.
- **Erfordert Administratorrechte** bei jeder Ausführung, da es Einstellungen auf Systemebene ändert.
- Perfekt für Privatanwender, Datenschutzaudits und einzelne Arbeitsplätze.

➡️ Mehr über die Free Edition erfahren

Premium Edition — *Bleiben Sie privat. Für immer.*

Die **Premium Edition** ist für professionelle und Unternehmensumgebungen konzipiert. Sie verwendet eine Client/Service-Architektur, die automatischen und proaktiven Datenschutz bietet — und sicherstellt, dass Ihre Einstellungen auch nach Windows-Updates durchgesetzt werden.

- Verwendet ein **Client/Service-Modell** — der Dienst läuft im Hintergrund und wendet Einstellungen automatisch an.
- **Proaktiver Schutz** — wendet Ihre bevorzugten Einstellungen automatisch nach Windows-Updates oder Richtlinienänderungen erneut an.
- **Erfordert keine Administrator-Rechte für Endbenutzer** — der Hintergrunddienst übernimmt alle privilegierten Operationen.

- Ideal für Unternehmensumgebungen, verwaltete Arbeitsplätze und IT-Abteilungen.

➡️ Mehr über die Premium Edition erfahren

So verwenden Sie diese Dokumentation

Nutzen Sie die Seitenleisten-Navigation, um Funktionen zu erkunden und detaillierte Informationen zu finden:

- Die Abschnitte **Free Edition** und **Premium Edition** beschreiben die spezifischen Funktionen und Arbeitsabläufe jeder Edition.
- Der Abschnitt **Funktionen** behandelt alle Datenschutz- und Konfigurationseinstellungen. Funktionen, die ausschließlich der Premium Edition vorbehalten sind, sind mit einem Premium-Badge gekennzeichnet.

Funktionsvergleich

O&O ShutUp10 ist in zwei Editionen erhältlich. Die **Free Edition** ist ein portables, interaktives Datenschutz-Tool für Einzelbenutzer. Die **Premium Edition** ergänzt eine Client/Service-Architektur mit automatischer Durchsetzung und ist damit für professionelle und Unternehmensumgebungen geeignet.

Diese Seite bietet einen detaillierten Vergleich beider Editionen und erklärt, warum O&O ShutUp10 eine zuverlässigere Datenschutzdurchsetzung als Gruppenrichtlinienobjekte (GPO) bietet.

Vergleichstabelle der Editionen

Funktion	Free Edition	Premium Edition
Datenschutzeinstellungsverwaltung (~300 Einstellungen)	✅	✅
Empfehlungsstufen für jede Einstellung	✅	✅
Systemwiederherstellungspunkte erstellen und wiederherstellen	✅	✅
Empfohlene Einstellungen in einem Schritt anwenden/rückgängig machen	✅	✅
Profile und Export/Import	✅	✅
KI-Entfernung (Copilot & Recall)	✅	✅
Bearbeitungsmodus für fortgeschrittene Benutzer	✅	✅
Portabel — keine Installation erforderlich	✅	—
Client/Service-Architektur	—	✅
Automatische Neuanwendung nach Windows-Updates	—	✅
Automatische Neuanwendung nach Gruppenrichtlinienänderungen	—	✅
Kontinuierliche Hintergrundüberwachung	—	✅
Keine Endbenutzer-Administratorrechte erforderlich	—	✅
Profil-Editor für zentrale Richtlinienverwaltung	—	✅
Geeignet für Unternehmenseinsatz	—	✅

Was die Premium Edition hinzufügt

Automatischer Schutz

Der bedeutendste Vorteil der Premium Edition ist der **Automatische Schutz**. Die Free Edition wendet Einstellungen nur an, wenn ein Benutzer die Anwendung manuell ausführt — wenn ein Windows-Update oder eine Richtlinienänderung diese Einstellungen zurücksetzt, muss der Benutzer sie manuell überprüfen und erneut anwenden.

Die Premium Edition führt einen Hintergrunddienst aus, der datenschutzrelevante Registry-Werte **kontinuierlich überwacht**. Wenn er erkennt, dass eine Einstellung geändert wurde — sei es durch ein Windows-Update, eine Gruppenrichtlinien-Aktualisierung oder eine andere Systemänderung — **wendet er die bevorzugte Konfiguration automatisch erneut an**, ohne Benutzereingriff.

➡️ Mehr über den Automatischen Schutz erfahren

Client/Service-Architektur

Die Premium Edition trennt die Benutzeroberfläche (Client) von der Durchsetzungs-Engine (Dienst):

- **Der Dienst** läuft als Windows-Dienst mit Systemrechten und übernimmt alle privilegierten Operationen im Hintergrund.
- **Der Client** ist eine Standard-Benutzeranwendung, die mit dem Dienst kommuniziert — keine Administratorrechte erforderlich.

Diese Architektur ist unverzichtbar in Unternehmensumgebungen, in denen Endbenutzer keine Admin-Rechte haben. Die Free Edition erfordert dagegen bei jeder Ausführung Administratorrechte.

Profil-Editor

Die Premium Edition enthält einen **Profil-Editor**, der IT-Administratoren ermöglicht, standardisierte Datenschutzkonfigurationen über mehrere Arbeitsplätze hinweg zu erstellen, zu bearbeiten und bereitzustellen. Dies ermöglicht eine zentrale Richtlinienverwaltung, ohne dass jeder Benutzer Einstellungen einzeln konfigurieren muss.

➡️ Mehr über den Profil-Editor erfahren

Warum O&O ShutUp10 GPO bei der Datenschutzdurchsetzung überlegen ist

Viele IT-Administratoren setzen auf Gruppenrichtlinienobjekte (GPO) zur Verwaltung von Windows-Datenschutzeinstellungen. Obwohl GPO ein leistungsstarkes Werkzeug für die Systemkonfiguration ist, hat es gut dokumentierte Einschränkungen bei der **dauerhaften Durchsetzung von Datenschutzeinstellungen** — insbesondere über Windows-Updates hinweg.

Das Problem: Windows-Updates können GPO-verwaltete Datenschutzeinstellungen zurücksetzen

Microsofts kumulative und Feature-Updates setzen bekanntermaßen datenschutzrelevante Einstellungen zurück oder überschreiben sie, selbst wenn diese zuvor über Gruppenrichtlinien konfiguriert wurden. Dieses Verhalten wurde in mehreren Kontexten dokumentiert:

- **Feature-Updates setzen lokale und registry-basierte Datenschutzeinstellungen zurück.** Große Windows-Feature-Updates (z.B. halbjährliche Kanalversionen) können datenschutzrelevante Registry-Werte und lokale Gruppenrichtlinieneinstellungen auf ihre Standards zurücksetzen. Microsofts eigene Dokumentation bestätigt, dass Feature-Updates effektiv ein In-Place-Upgrade durchführen, das frühere Konfigurationen überschreiben kann. (Microsoft Learn — Übersicht Windows-Feature-Updates)
- **Die GPO-Neuanwendung hängt vom Richtlinien-Aktualisierungszyklus ab.** Selbst bei domänenbasierten GPOs werden Einstellungen nur während des Gruppenrichtlinien-Aktualisierungsintervalls erneut angewendet (typischerweise alle 90 Minuten

± 30 Minuten für Computereinstellungen). Zwischen einem Windows-Update, das einen Wert zurücksetzt, und der nächsten GPO-Aktualisierung läuft das System mit Standard-Einstellungen (weniger privat). (Microsoft Learn — Gruppenrichtlinienverarbeitung))

- **Nicht alle Datenschutzeinstellungen sind über Gruppenrichtlinien zugänglich.** Einige Windows-Datenschutz- und Telemetrieeinstellungen können nur über direkte Registry-Änderung konfiguriert werden und haben keine entsprechende administrative Gruppenrichtlinienvorlage. GPO kann keine Einstellungen durchsetzen, die nicht in seinen ADMX/ADML-Vorlagen dargestellt sind. (Microsoft Learn — Verbindungen von Windows zu Microsoft-Diensten verwalten)
- **Lokale Gruppenrichtlinien (ohne Domäne) sind besonders anfällig.** Computer, die keiner Active Directory-Domäne angehören, sind auf lokale Gruppenrichtlinien angewiesen, die noch anfälliger dafür sind, während Feature-Updates überschrieben zu werden. Lokale Richtlinieneinstellungen, die in der Registry unter `HKLM\SOFTWARE\Policies` gespeichert sind, können durch den Update-Prozess gelöscht oder zurückgesetzt werden.

Wie O&O ShutUp10 Premium dieses Problem löst

Der Automatische Schutz von O&O ShutUp10 Premium adressiert jede dieser Einschränkungen:

GPO-Einschränkung	O&O ShutUp10 Premium
Einstellungen können durch Windows-Feature-Updates zurückgesetzt werden	Der Hintergrunddienst erkennt Änderungen und wendet Einstellungen **sofort** erneut an — ohne auf einen Richtlinien-Aktualisierungszyklus zu warten.
GPO-Aktualisierung erfolgt nur alle ~90 Minuten	Der Dienst überwacht Registry-Werte **kontinuierlich** und reagiert auf Änderungen in Echtzeit.
Einige Datenschutzeinstellungen haben kein GPO-Äquivalent	O&O ShutUp10 verwaltet Einstellungen durch direkte Registry-Änderung und deckt Einstellungen ab, die **keine ADMX/ADML-Vorlage** haben.
Lokale Gruppenrichtlinien werden durch Feature-Updates überschrieben	Der Dienst speichert die gewünschte Konfiguration unabhängig von Gruppenrichtlinien, sodass er Einstellungen **unabhängig davon, was der Update-Prozess ändert** erneut anwenden kann.
Erfordert Active Directory-Infrastruktur für Domänen-GPO	O&O ShutUp10 funktioniert auf **eigenständigen Rechnern** und domänenverbundenen Rechnern gleichermaßen — keine AD-Infrastruktur erforderlich.

Wann GPO weiterhin angemessen ist

Gruppenrichtlinien bleiben das richtige Werkzeug für viele Systemkonfigurationsaufgaben — Softwarebereitstellung, Sicherheitsbaselines, Laufwerkszuordnungen und Anmeldeskripte, unter anderem. Der obige Punkt bezieht sich speziell auf **Datenschutz- und Telemetrieeinstellungen**, bei denen die Kombination aus häufigen Windows-Updates und unvollständiger ADMX-Abdeckung die GPO-Durchsetzung ohne ein ergänzendes Tool unzuverlässig macht.

O&O ShutUp10 Premium kann **neben** Gruppenrichtlinien als ergänzende Durchsetzungsebene arbeiten und sicherstellen, dass Datenschutzeinstellungen konsistent bleiben, auch wenn GPO allein dies nicht garantieren kann.

Referenzen

1. Microsoft Learn — *How Windows Update works*: https://learn.microsoft.com/en-us/windows/deployment/update/how-windows-update-works
2. Microsoft Learn — *Group Policy processing and precedence*: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11))

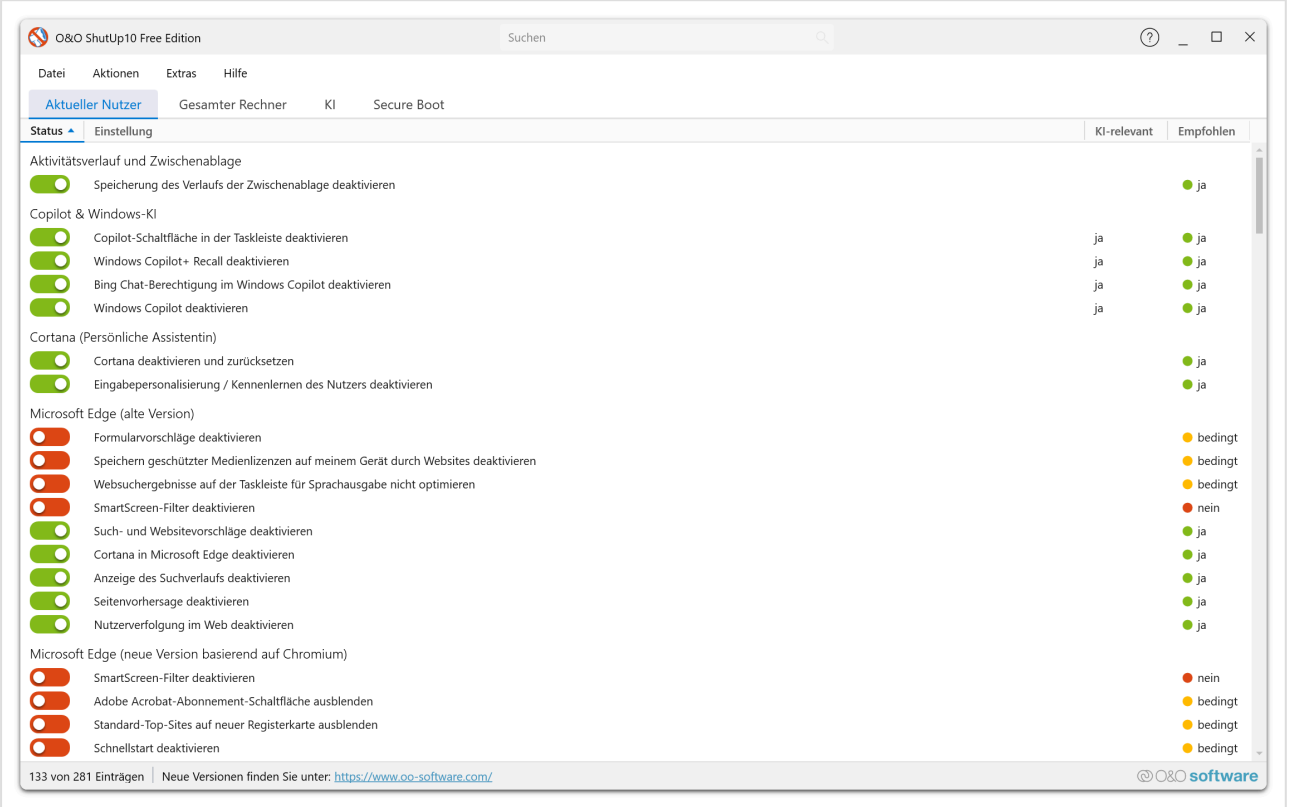
3. Microsoft Learn — *Manage connections from Windows operating system components to Microsoft services*: https://learn.microsoft.com/en-us/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

Zusammenfassung

	Nur GPO	O&O ShutUp10 Free	O&O ShutUp10 Premium
Deckt alle Windows-Datenschutzeinstellungen ab	Teilweise	✅	✅
Übersteht Windows-Feature-Updates automatisch	❌	❌ (manuelle Überprüfung)	✅
Kontinuierliche Überwachung und Neuanwendung	❌	❌	✅
Funktioniert ohne Active Directory	Nur lokale GPO	✅	✅
Keine Admin-Rechte für Endbenutzer nötig	Abhängig vom Setup	❌	✅
Zentrale Profilverwaltung	Über AD/GPO	Export/Import	✅ Profil-Editor

O&O ShutUp10 Free Edition

Die **Free Edition** von O&O ShutUp10 ist ein leistungsstarkes, portables Datenschutz-Tool für Windows 10 und Windows 11. Es gibt Ihnen sofortige, vollständige Kontrolle über Ihre Windows-Datenschutzeinstellungen — ohne Installation, Abonnements oder technisches Fachwissen. Einfach herunterladen, ausführen und die Kontrolle über Ihre Daten übernehmen.



So funktioniert es

Die O&O ShutUp10 Free Edition läuft als eigenständige portable Anwendung. Beim Start scannt sie Ihre aktuellen Windows-Datenschutz- und Telemetrieeinstellungen und stellt sie in einer übersichtlichen Liste mit klaren Umschaltern dar.

1. **Laden** Sie die Anwendung von der O&O Software-Website herunter.
2. **Führen** Sie sie direkt aus — keine Installation erforderlich.
3. **Überprüfen** Sie die Liste der Datenschutzeinstellungen, jede mit einer Empfehlungsstufe.
4. **Schalten** Sie Einstellungen ein oder aus, um Ihre Datenschutzpräferenzen anzupassen.
5. **Übernehmen** Sie Ihre Änderungen und schließen Sie die Anwendung.

> **Info**
>
> **Administratorrechte erforderlich:** Die Free Edition erfordert immer Administratorrechte, da sie Windows-Systemeinstellungen und Registry-Werte direkt ändert. Sie werden bei jedem Start von der Windows-Benutzerkontensteuerung (UAC) dazu aufgefordert.

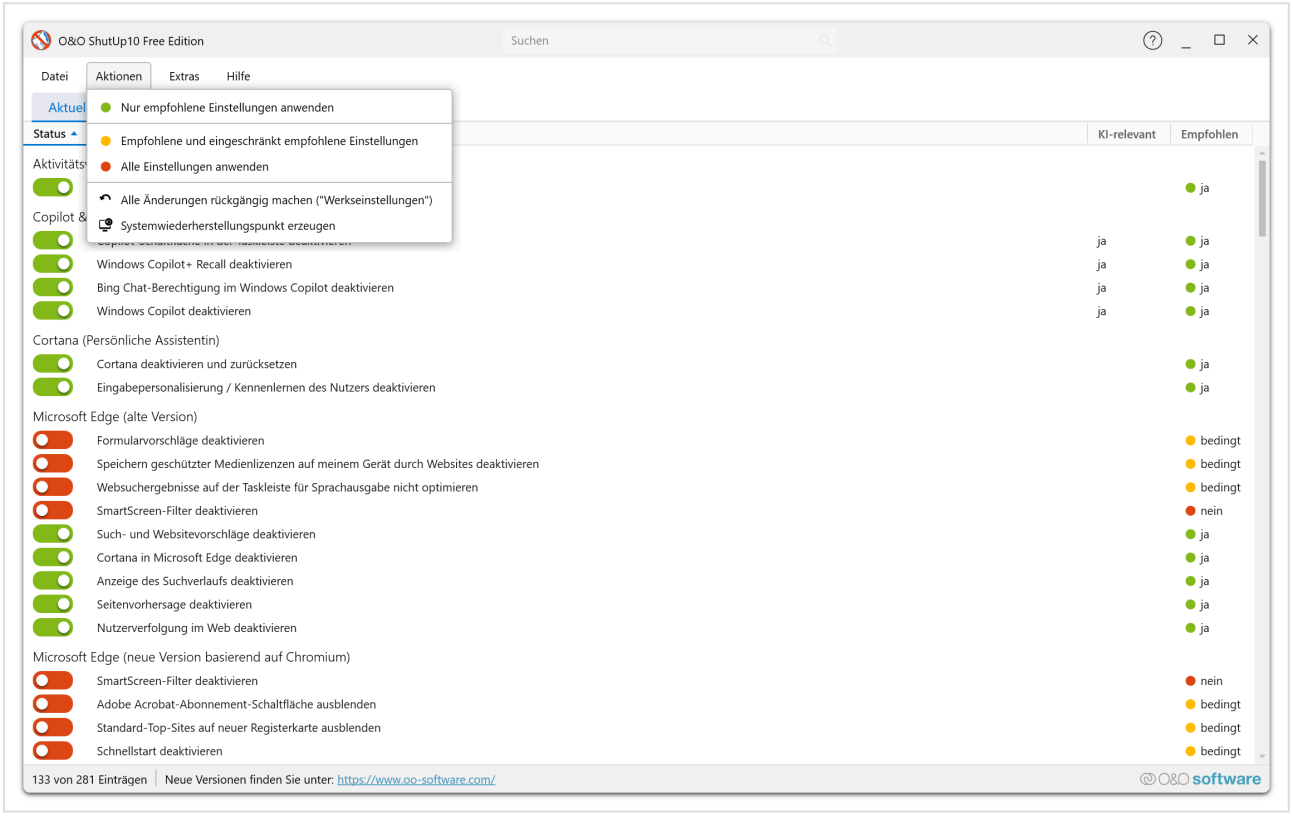
Wichtige Funktionen

Portable Anwendung

Keine Installation, keine Hintergrunddienste, keine Rückstände. Einfach herunterladen, ausführen und Ihre Datenschutzeinstellungen verwalten. Ideal für USB-Laufwerke und einmalige Datenschutzaudits.

Interaktive Datenschutzverwaltung

Jede Änderung wird interaktiv vom Benutzer vorgenommen. Sie überprüfen jede Einstellung, sehen ihren aktuellen Status und entscheiden, ob Sie sie aktivieren oder deaktivieren möchten. Nichts ändert sich ohne Ihre ausdrückliche Aktion.



Empfehlungsstufen

Jeder Einstellung ist eine Empfehlungsstufe zugeordnet, die Ihnen bei der Entscheidung hilft:

- **Empfohlen** — Sicher für die meisten Benutzer anzuwenden; keine negativen Auswirkungen auf die Funktionalität.
- **Eingeschränkt empfohlen** — Grundsätzlich sicher, kann aber bestimmte Funktionen beeinträchtigen.
- **Nicht empfohlen** — Kann wichtige Windows-Funktionalität beeinträchtigen; nur anwenden, wenn Sie die Konsequenzen verstehen.

Systemwiederherstellungspunkte erstellen und wiederherstellen

Vor dem Vornehmen von Änderungen können Sie einen Systemwiederherstellungspunkt erstellen. Falls etwas nicht wie erwartet funktioniert, können Sie alle Änderungen einfach rückgängig machen.

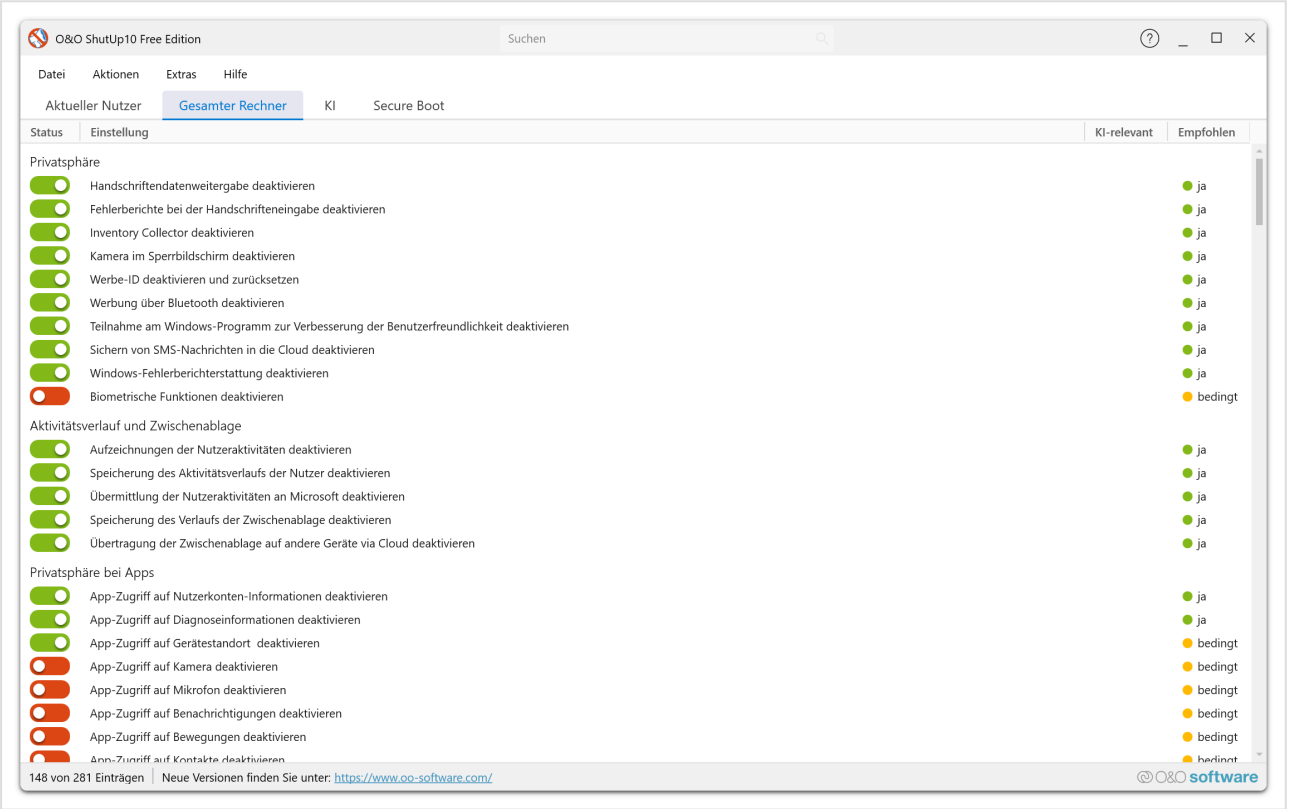
Empfohlene Einstellungen anwenden

Wenden Sie alle empfohlenen Einstellungen auf einmal an, anstatt jede einzeln umzuschalten. Sie können auch alle Änderungen rückgängig machen oder alles auf Windows-Standards zurücksetzen.

Registerkarten „Aktueller Benutzer" und „Lokaler Computer"

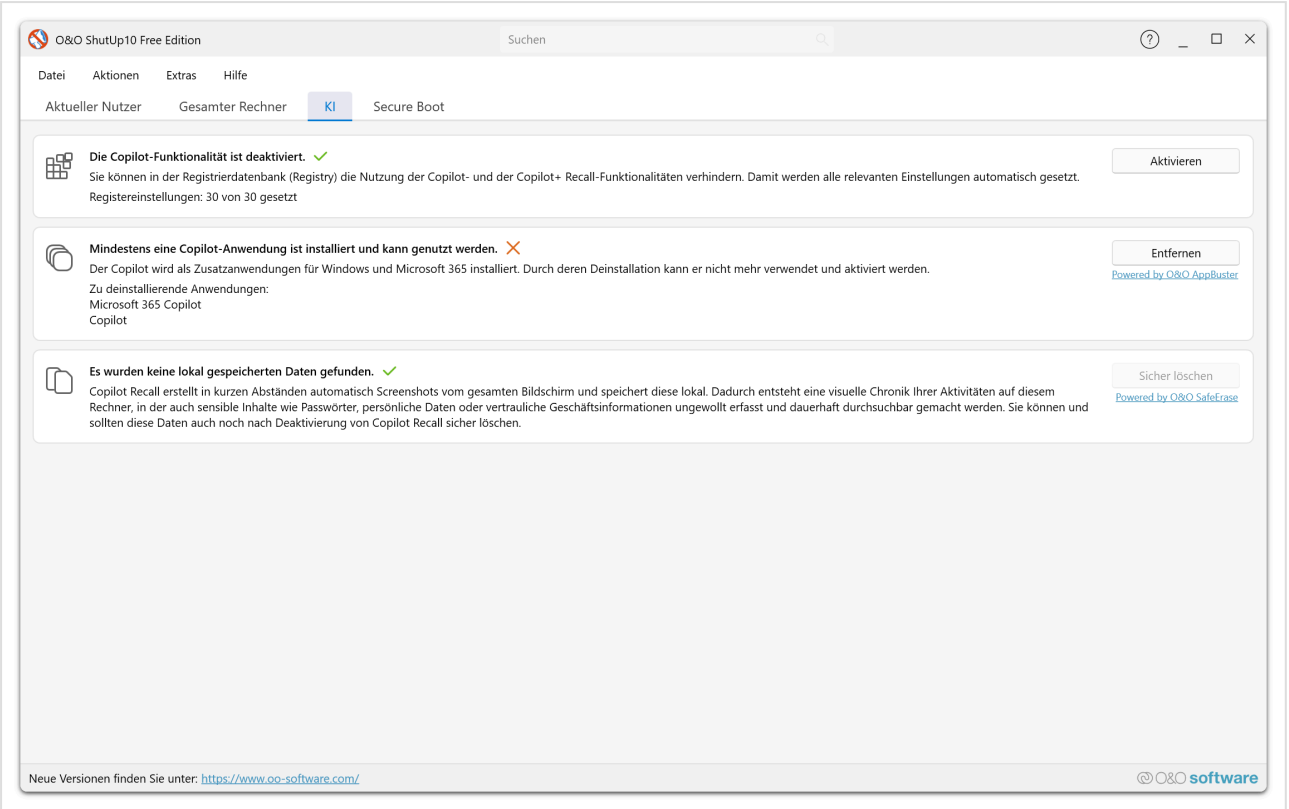
Die Free Edition organisiert Datenschutzeinstellungen in zwei Hauptbereiche:

- **Aktueller Benutzer** — Einstellungen, die für das aktuell angemeldete Windows-Benutzerkonto gelten (z.B. Datenschutzeinstellungen, App-Berechtigungen, Werbe-ID).
- **Lokaler Computer** — Einstellungen, die systemweit für alle Benutzer auf dem Computer gelten (z.B. Telemetrie, Fehlerberichterstattung, Bluetooth-Werbung).



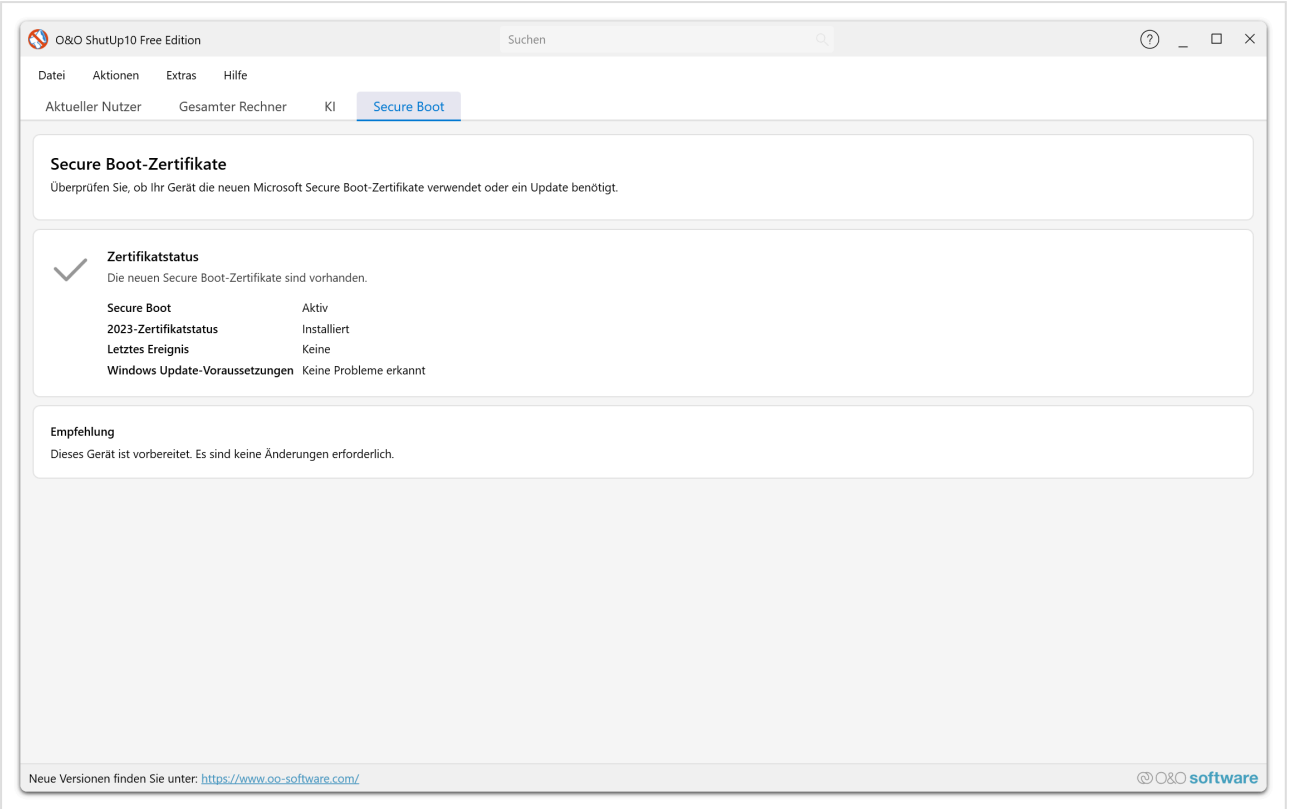
KI-Entfernung

Die Free Edition enthält die vollständige KI-Entfernungsfunktion zum Deaktivieren von Microsoft Copilot und Recall-Komponenten. Die Registerkarte **KI** bietet einen dreistufigen Ansatz: Deaktivierung KI-bezogener Registry-Einstellungen, Entfernung von Copilot-Anwendungen und sichere Löschung von Recall-Daten.



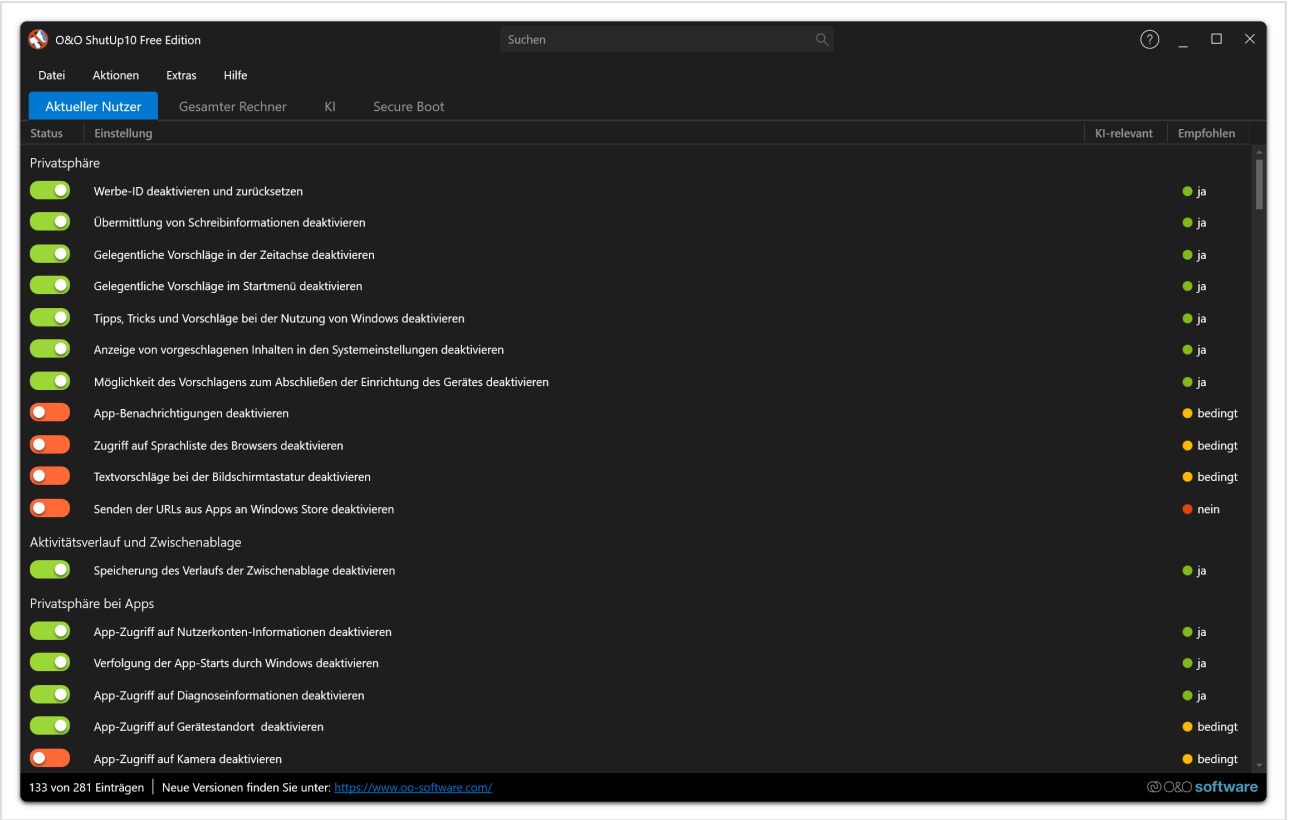
Secure Boot-Zertifikate

Die Registerkarte **Secure Boot** prüft, ob Ihr Gerät die neuesten Microsoft Secure Boot-Zertifikate verwendet oder ein Update benötigt. Sie zeigt den Zertifikatstatus, letzte Ereignisinformationen und eine Empfehlung für erforderliche Maßnahmen an.



Unterstützung für dunklen Modus

Die Free Edition unterstützt helle und dunkle Designthemen. Der Anzeigemodus folgt standardmäßig Ihrer Windows-Systemeinstellung, oder Sie können einen bestimmten Modus im Einstellungsdialog auswählen.



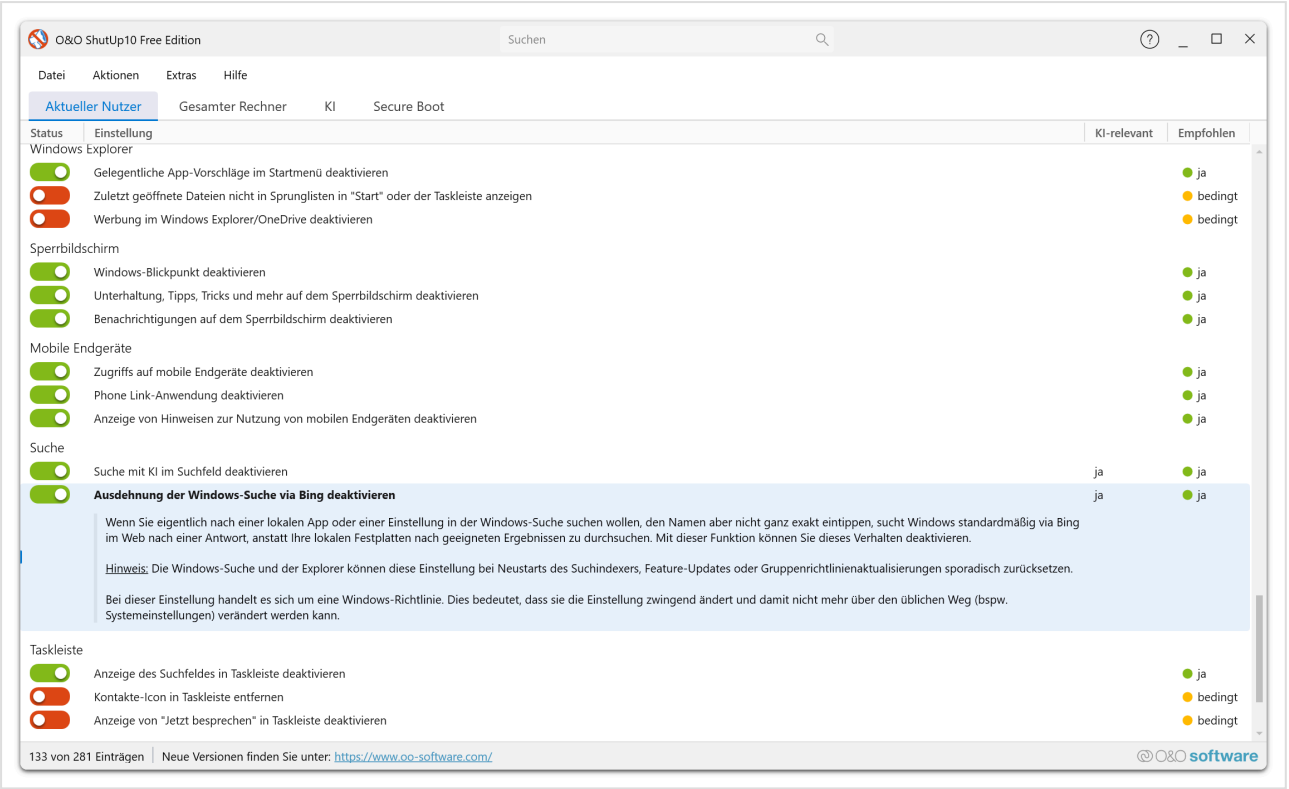
Einstellungskategorien

Die Free Edition deckt alle wichtigen Datenschutzeinstellungskategorien ab:

- Datenschutzeinstellungen
- Telemetrie und Datenerfassung
- Standortdienste
- Cortana und Suche
- Windows Update-Verhalten
- App-Berechtigungen und -Zugriff
- Windows Explorer und Werbung
- Sicherheitsrelevante Einstellungen

Einstellungsdetails

Klicken Sie auf eine beliebige Einstellung, um ihre Beschreibung zu erweitern. Die erweiterte Ansicht zeigt eine detaillierte Erklärung der Funktion, ihre möglichen Auswirkungen und Hinweise, z.B. ob ein Systemneustart nach der Änderung erforderlich ist.



Informationen zur Dateigröße

Wenn Sie die Free Edition erstmals herunterladen, fällt Ihnen möglicherweise auf, dass sie größer ist als ältere Versionen. Die Anwendung zeigt einen Informationsdialog an, der diese Änderung erklärt:

Die erhöhte Dateigröße ist beabsichtigt: Alle Laufzeitkomponenten, die zuvor von Windows bereitgestellt wurden, sind jetzt direkt in die ausführbare Datei eingebettet. Dies stellt sicher, dass die Anwendung auf jedem System zuverlässig funktioniert, ohne von vorinstallierten Frameworks abhängig zu sein. Die Funktionalität bleibt identisch — nur die Paketierung hat sich geändert.

Für wen ist die Free Edition geeignet?

Die Free Edition ist die ideale Wahl für jeden, der sofortige, kompromisslose Datenschutzkontrolle wünscht:

- **Privatanwender**, die eine schnelle, effektive Möglichkeit zur Kontrolle ihrer Windows-Datenschutzeinstellungen suchen.
- **Technische Benutzer**, die Datenschutzaudits auf einzelnen Rechnern durchführen.
- **IT-Fachleute**, die ein portables Tool zur Stichprobenprüfung von Datenschutzkonfigurationen benötigen.
- **Datenschutzbewusste Benutzer**, die eine bewährte, vertrauenswürdige Lösung ohne Kostenbarrieren wünschen.

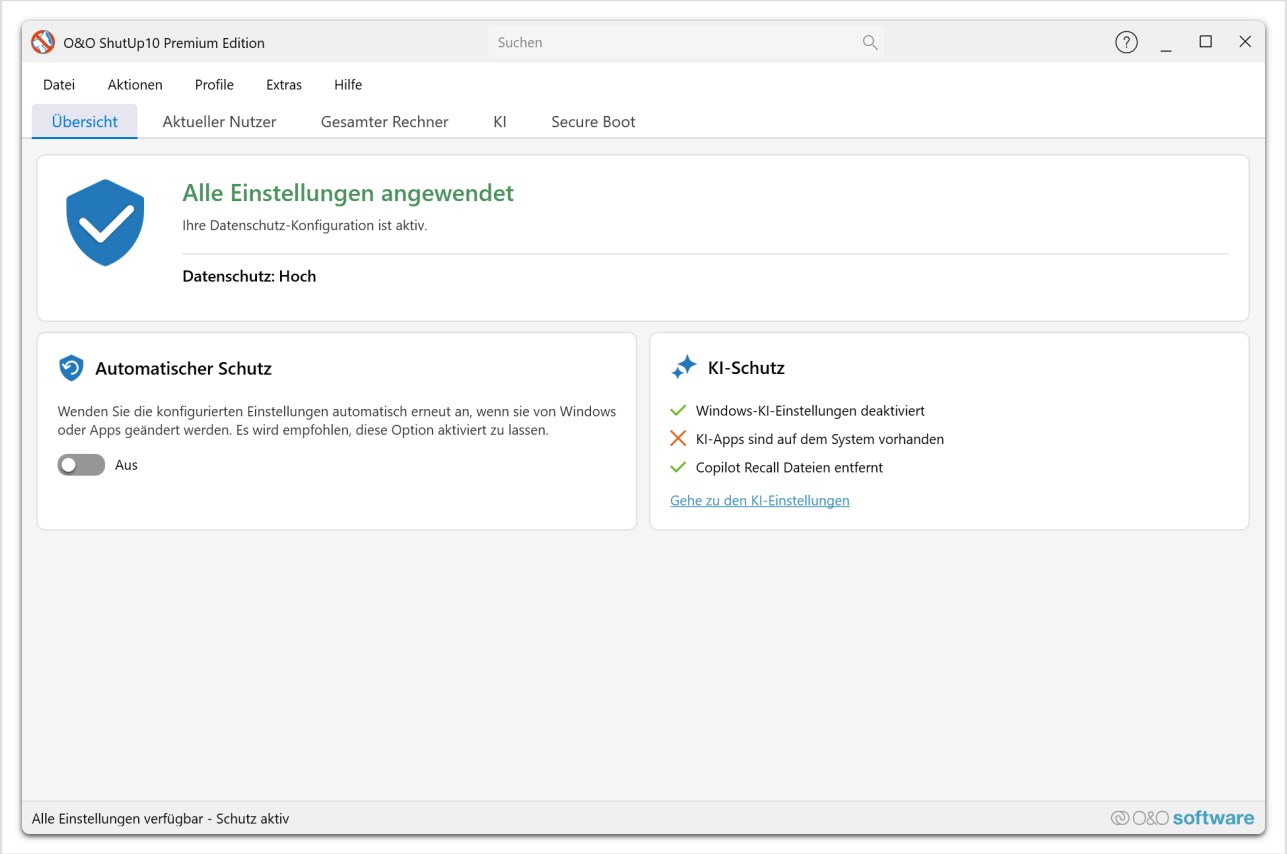
Die Free Edition bietet die gleiche umfassende Abdeckung der Datenschutzeinstellungen wie die Premium Edition — fast 300 Einstellungen — und ist damit eine vollständige Datenschutzlösung für den individuellen Gebrauch.

Für Umgebungen, die automatischen Schutz oder den Betrieb ohne Administrator-Rechte für Endbenutzer erfordern, siehe die Premium Edition.

O&O ShutUp10 Premium Edition

> **Bleiben Sie privat. Für immer.**

Die **Premium Edition** von O&O ShutUp10 ist für professionelle und Unternehmensumgebungen konzipiert. Sie verwendet eine Client/Service-Architektur, die automatischen, kontinuierlichen Datenschutz bietet — ohne dass Endbenutzer-Administratorrechte erforderlich sind.

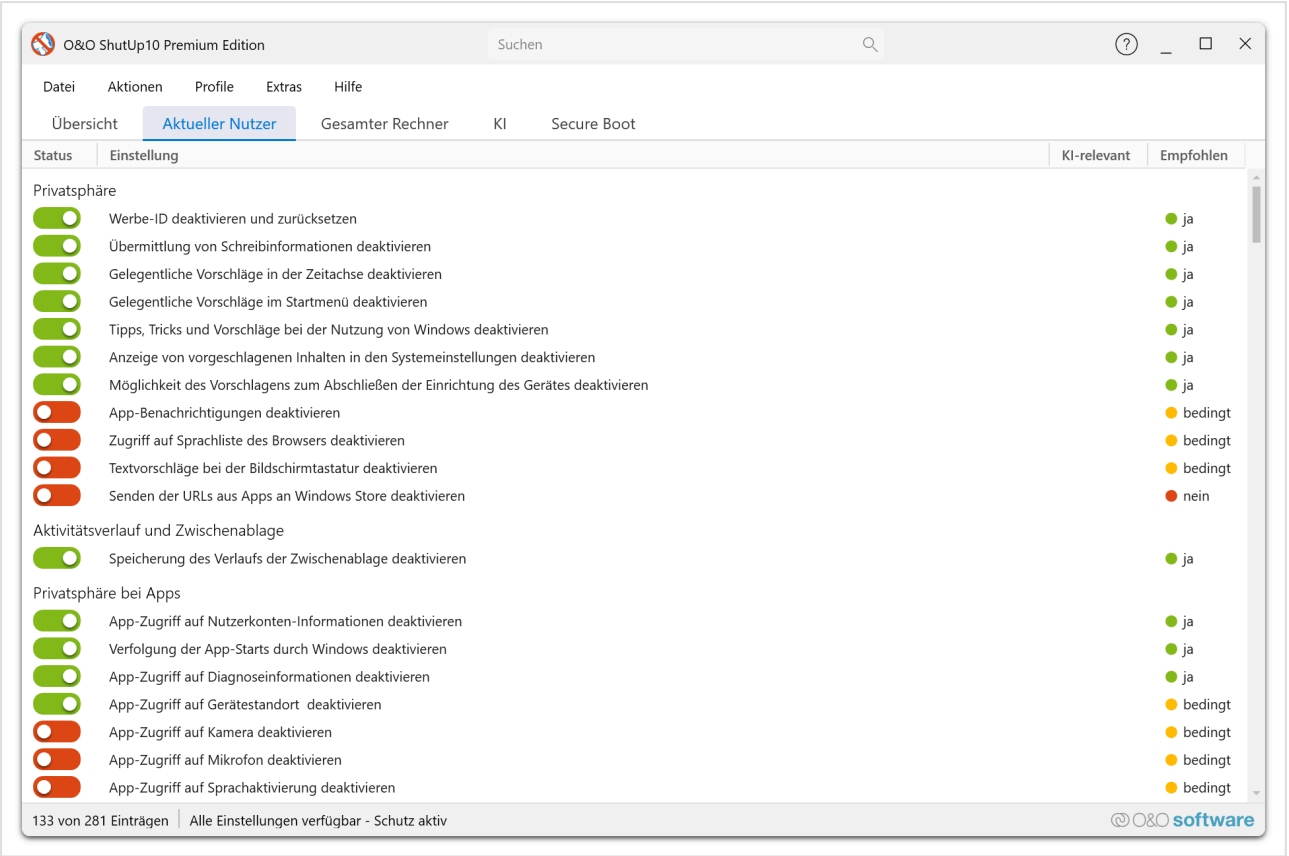


So funktioniert es

Die Premium Edition besteht aus zwei Komponenten:

1. **Der Dienst** — Ein Windows-Dienst, der im Hintergrund mit den notwendigen Systemrechten läuft. Er überwacht und wendet Ihre Datenschutzeinstellungen automatisch an.
2. **Der Client** — Eine benutzerorientierte Anwendung, die mit dem Dienst kommuniziert. Benutzer können Einstellungen anzeigen und konfigurieren, ohne Administratorrechte zu benötigen.

Diese Trennung bedeutet, dass der Dienst alle privilegierten Operationen übernimmt, während Endbenutzer mit der Client-Anwendung über ihr Standard-Windows-Konto interagieren.



Wichtige Funktionen

Client/Service-Architektur

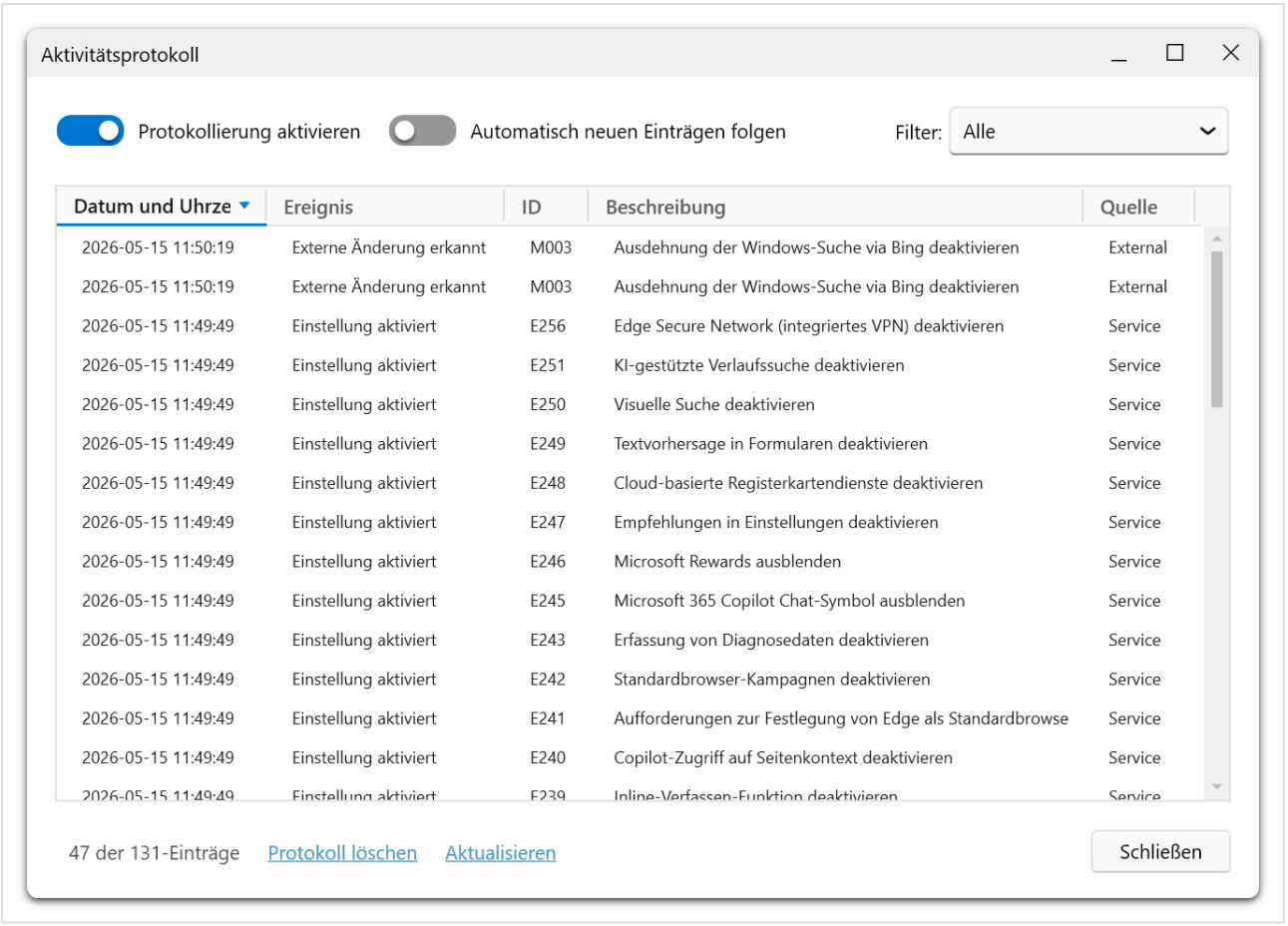
Im Gegensatz zur Free Edition, die bei jeder Ausführung Administratorrechte erfordert, führt die Premium Edition einen Hintergrunddienst aus, der die notwendigen Berechtigungen besitzt. Endbenutzer interagieren über den Client ohne erhöhte Berechtigungen.

Proaktiver Schutz

Der Dienst überwacht kontinuierlich Ihre Datenschutzeinstellungen und wendet Ihre bevorzugte Konfiguration automatisch nach folgenden Ereignissen erneut an:

- **Windows-Updates**, die Datenschutzeinstellungen möglicherweise zurücksetzen.
- **Gruppenrichtlinienänderungen**, die lokale Einstellungen überschreiben.
- **Systemkonfigurationsänderungen**, die datenschutzrelevante Registry-Werte betreffen.

Dies stellt sicher, dass Ihre Datenschutzeinstellungen über die Zeit konsistent bleiben, ohne manuellen Eingriff.



Keine Endbenutzer-Administratorrechte erforderlich

In Unternehmensumgebungen haben die meisten Benutzer keine Admin-Rechte. Die Premium Edition löst dies, indem sie alle privilegierten Operationen an den Hintergrunddienst delegiert. Benutzer können ihre Datenschutzeinstellungen über den Client verwalten, ohne UAC-Eingabeaufforderungen oder Admin-Anmeldedaten.

Automatischer Schutz Premium

Legen Sie Ihre bevorzugte Datenschutzkonfiguration einmal fest, und der Dienst hält sie automatisch durchgesetzt. Benutzer müssen die Anwendung nicht erneut ausführen oder Einstellungen manuell überprüfen.

Alle Free Edition-Funktionen enthalten

Die Premium Edition enthält alle Funktionen der Free Edition, plus die oben beschriebenen zusätzlichen Möglichkeiten:

- Alle Datenschutzeinstellungskategorien (Telemetrie, Standort, Cortana, Windows Update, App-Berechtigungen usw.)
- Empfehlungsstufen für jede Einstellung
- Erstellung von Systemwiederherstellungspunkten
- Empfohlene Einstellungen in einem Schritt anwenden/rückgängig machen

Für wen ist die Premium Edition geeignet?

Die Premium Edition ist ideal für:

- **Unternehmensumgebungen**, in denen Benutzer keine Administratorrechte benötigen sollten.
- **IT-Abteilungen**, die konsistente Datenschutzrichtlinien über Arbeitsplatzflotten hinweg benötigen.
- **Organisationen**, die eine automatische Neuanwendung von Datenschutzeinstellungen nach Windows-Updates benötigen.
- **Managed Service Provider (MSPs)**, die Datenschutzkonfigurationen für mehrere Kunden pflegen.

Für den individuellen Gebrauch oder schnelle einmalige Datenschutzaudits kann die Free Edition ausreichend sein.

Erste Schritte

Diese Anleitung führt Sie durch den anfänglichen Einrichtungsprozess nach der Installation von O&O ShutUp10. Befolgen Sie diese Schritte, um mit der Free Edition oder der Premium Edition zu beginnen.

Free Edition — Erste Schritte

Die Free Edition erfordert keine Installation. Befolgen Sie diese Schritte, um mit der Verwaltung Ihrer Windows-Datenschutzeinstellungen zu beginnen:

1. Herunterladen und Starten

1. Laden Sie die O&O ShutUp10-Anwendung von der O&O Software-Website herunter.
2. Führen Sie die Anwendung direkt aus — keine Installation erforderlich.
3. Windows zeigt eine **Benutzerkontensteuerung (UAC)**-Eingabeaufforderung an. Klicken Sie auf **Ja**, um Administratorrechte zu gewähren.

> **Info**
>
> Die Free Edition erfordert immer Administratorrechte, da sie Windows-Systemeinstellungen und Registry-Werte direkt ändert.

2. Datenschutzeinstellungen überprüfen

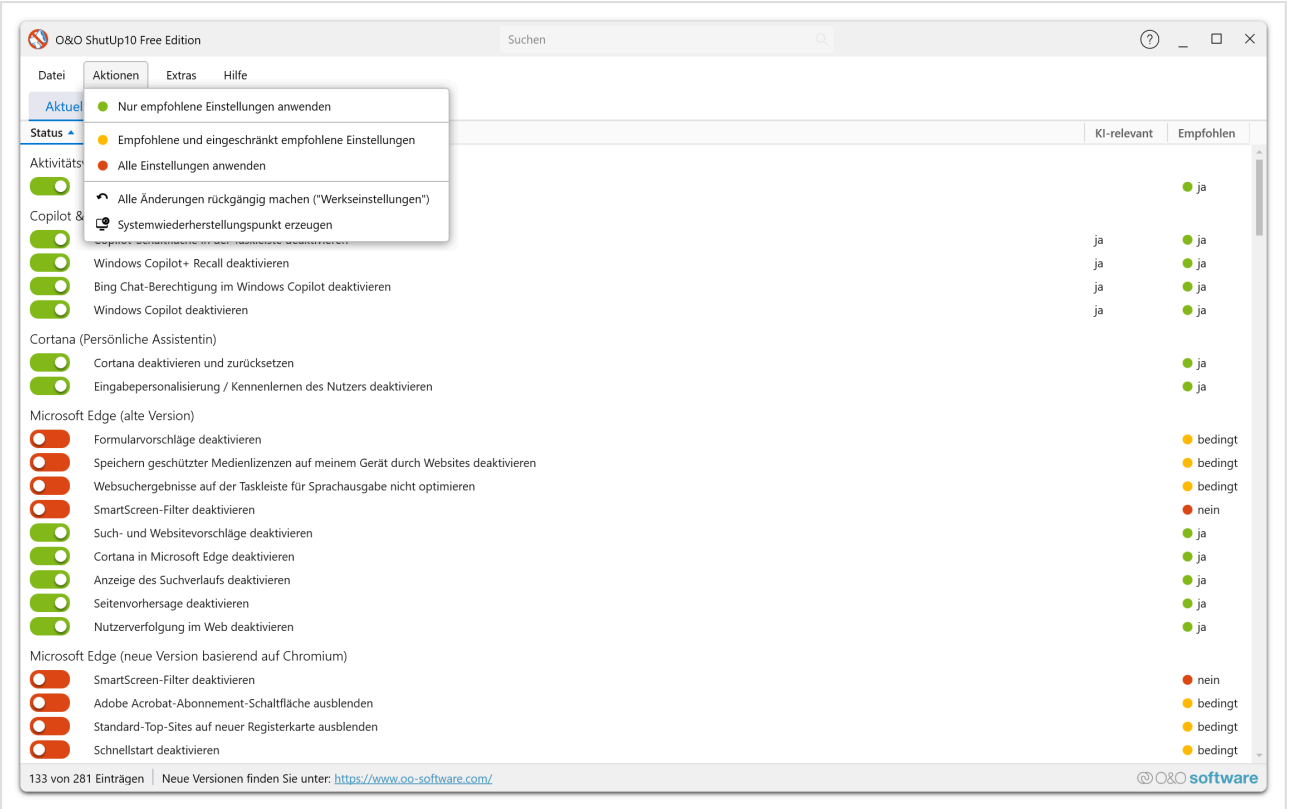
Nach dem Start scannt O&O ShutUp10 Ihre aktuellen Windows-Datenschutz- und Telemetrieeinstellungen. Das Hauptfenster zeigt eine kategorisierte Liste aller verfügbaren Einstellungen, jeweils mit:

- Einem **Umschalter**, der den aktuellen Status anzeigt (aktiviert oder deaktiviert).
- Einer **Empfehlungsstufe** — Empfohlen, Eingeschränkt oder Nicht empfohlen.

Nehmen Sie sich einen Moment Zeit, um die Einstellungen und ihre Empfehlungsstufen zu überprüfen, bevor Sie Änderungen vornehmen.

3. Systemwiederherstellungspunkt erstellen

Erstellen Sie vor dem Vornehmen von Änderungen einen Systemwiederherstellungspunkt über das **Aktionen**-Menü:



1. Öffnen Sie **Aktionen → Systemwiederherstellungspunkt erstellen**.
2. Bestätigen Sie die Erstellung, wenn Sie dazu aufgefordert werden.

Dies ermöglicht es Ihnen, alle Änderungen rückgängig zu machen, falls etwas nicht wie erwartet funktioniert.

4. Empfohlene Einstellungen anwenden

Für einen schnellen Start wenden Sie alle empfohlenen Einstellungen auf einmal an:

1. Öffnen Sie **Aktionen → Alle empfohlenen Einstellungen anwenden**.
2. Bestätigen Sie die Aktion, wenn Sie dazu aufgefordert werden.

Dies aktiviert alle als **Empfohlen** markierten Einstellungen — sicher für die meisten Benutzer mit minimaler Auswirkung auf die Windows-Funktionalität.

5. Einzelne Einstellungen anpassen

Nach dem Anwenden der empfohlenen Einstellungen überprüfen Sie die verbleibenden Einstellungen und passen Sie sie nach Ihren Wünschen an:

- **Eingeschränkt empfohlene** Einstellungen sind grundsätzlich sicher, können aber bestimmte Funktionen beeinträchtigen.
- **Nicht empfohlene** Einstellungen können wichtige Windows-Funktionalität beeinträchtigen — nur anwenden, wenn Sie die Konsequenzen verstehen.

6. Anwendung schließen

Sobald Sie mit Ihren Einstellungen zufrieden sind, schließen Sie einfach die Anwendung. Ihre Änderungen werden in der Windows-Registry gespeichert und bleiben bestehen, bis sie von Ihnen, einem Windows-Update oder einer anderen Systemänderung

geändert werden.

> **Tip**
>
> Führen Sie O&O ShutUp10 nach jedem größeren Windows-Update erneut aus, um zu überprüfen, dass Ihre Datenschutzeinstellungen nicht zurückgesetzt wurden.

Premium Edition — Erste Schritte

Die Premium Edition verwendet eine Client/Service-Architektur. Die Ersteinrichtung wird durch die **Premium-Übersicht**-Seite geführt, die Sie durch jeden Schritt leitet.

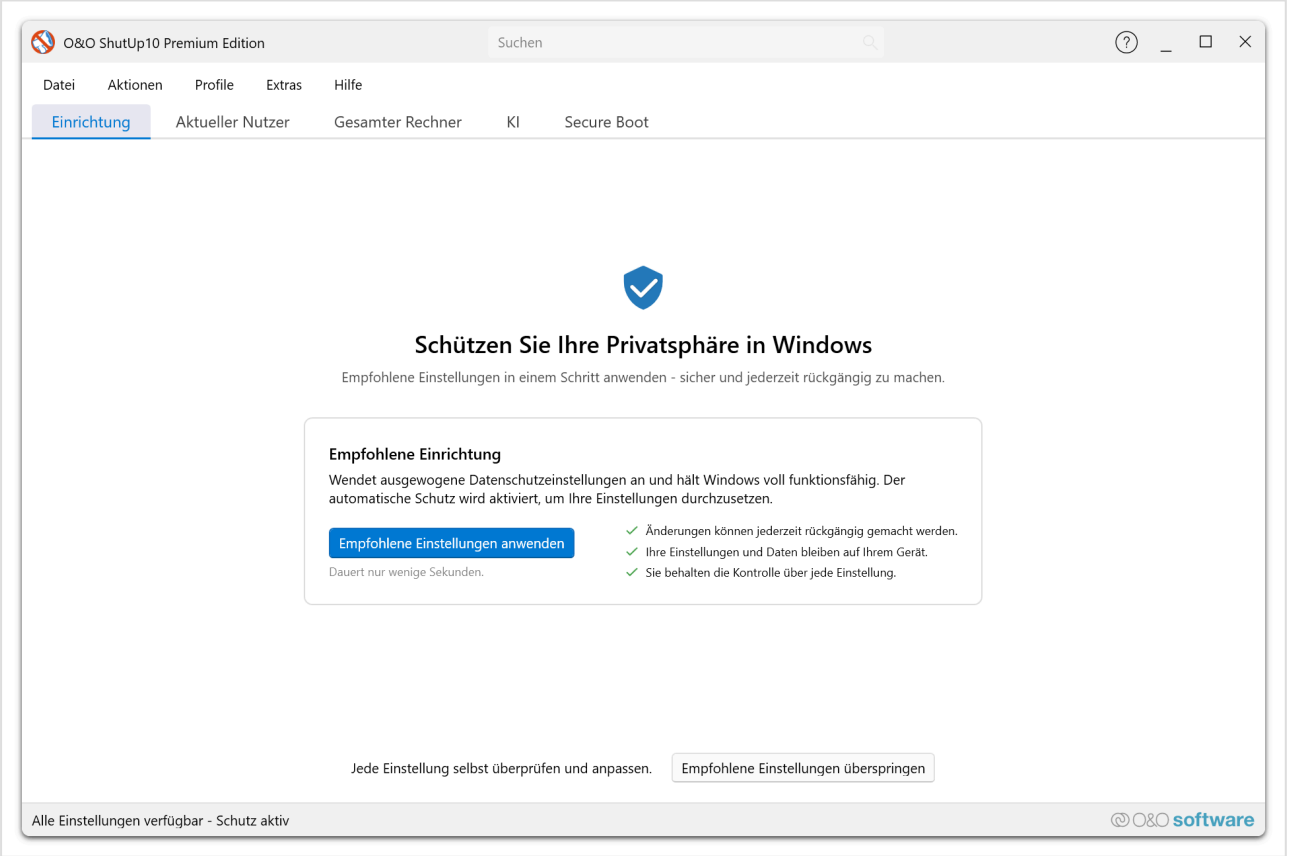
1. Premium Edition installieren

Installieren Sie die O&O ShutUp10 Premium Edition mit dem bereitgestellten Installationsprogramm. Das Installationsprogramm registriert:

- **Den Dienst** — Einen Windows-Hintergrunddienst, der mit Systemrechten läuft.
- **Den Client** — Die benutzerorientierte Anwendung zum Anzeigen und Konfigurieren von Einstellungen.

2. Client starten

Starten Sie nach der Installation die O&O ShutUp10 Client-Anwendung. Die **Premium-Übersicht** öffnet sich automatisch im **Setup-Modus**.



3. Geführtes Setup abschließen

Die Premium-Übersicht führt Sie im Setup-Modus durch die folgenden Schritte:

Schritt	Was passiert
Dienstinstallation	Das Setup überprüft, dass der Hintergrunddienst installiert und registriert ist.
Dienstverbindung	Der Client bestätigt die Kommunikation mit dem Hintergrunddienst.
Profilauswahl	Sie werden aufgefordert, ein erstes Datenschutzprofil auszuwählen (z.B. Empfohlene Einstellungen).
Erste Anwendung	Das ausgewählte Profil wird angewendet, um Ihre grundlegende Datenschutzkonfiguration festzulegen.

Es sind keine Administratorrechte vom Endbenutzer erforderlich — der Hintergrunddienst übernimmt alle privilegierten Operationen.

4. Schutzstatus überprüfen

Nach Abschluss des Setups wechselt die Premium-Übersicht in den **Übersichtsmodus** und zeigt an:

- **Schutzstatus** — Bestätigt, dass der automatische Schutz aktiv ist.
- **Dienststatus** — Zeigt, dass der Hintergrunddienst läuft.
- **Aktives Profil** — Zeigt den Namen des angewendeten Datenschutzprofils an.

5. Zusätzliche Einstellungen konfigurieren (Optional)

Nach der Ersteinrichtung können Sie die Anwendung über den **Einstellungsdialog** (**Ansicht** → **Einstellungen…**) weiter anpassen:

- **Benachrichtigungen** — Konfigurieren Sie, wie Sie über automatische Schutzereignisse benachrichtigt werden.
- **Autostart** — Legen Sie fest, dass die Anwendung beim Anmelden automatisch startet.
- **Hybrid-Modus** — Aktivieren Sie den automatischen Ausschluss von Einstellungen, die durch Gruppenrichtlinien verwaltet werden (nützlich in Unternehmensumgebungen).

Weitere Details finden Sie in der Dokumentation zum Einstellungsdialog.

6. Laufende Nutzung

Mit der Premium Edition werden Ihre Datenschutzeinstellungen automatisch gepflegt:

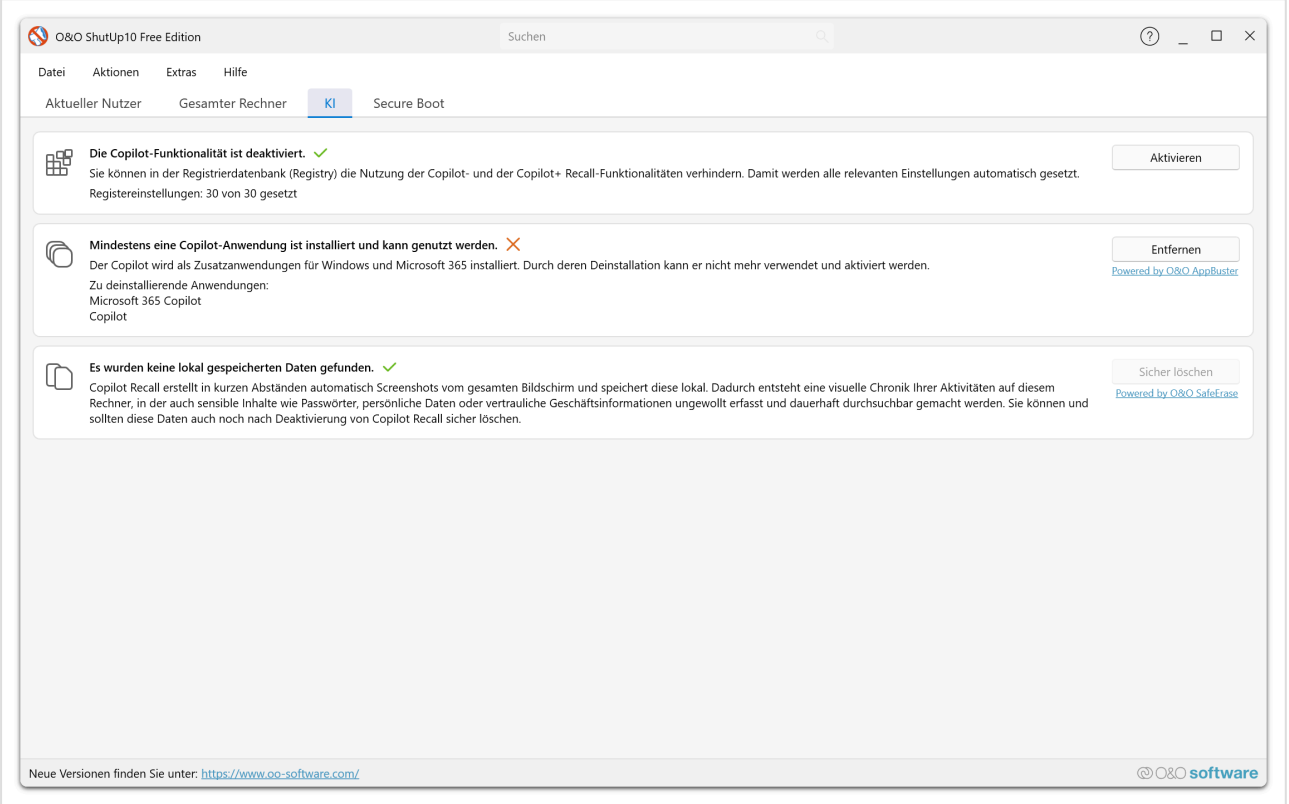
- Der Dienst überwacht kontinuierlich und wendet Ihre Konfiguration nach Windows-Updates, Gruppenrichtlinienänderungen oder Registry-Änderungen erneut an.
- Öffnen Sie den Client jederzeit, um den aktuellen Schutzstatus in der **Premium-Übersicht** zu prüfen.
- Verwenden Sie den Profil-Editor, um benutzerdefinierte Profile für verschiedene Szenarien zu erstellen und zu verwalten.

> **Tip**
>
> Wenn die Premium-Übersicht nach der Installation im Setup-Modus verbleibt, überprüfen Sie, ob der O&O ShutUp10-Dienst ausgeführt wird. Prüfen Sie die **Windows-Dienste** (services.msc) oder kontaktieren Sie Ihren IT-Administrator.

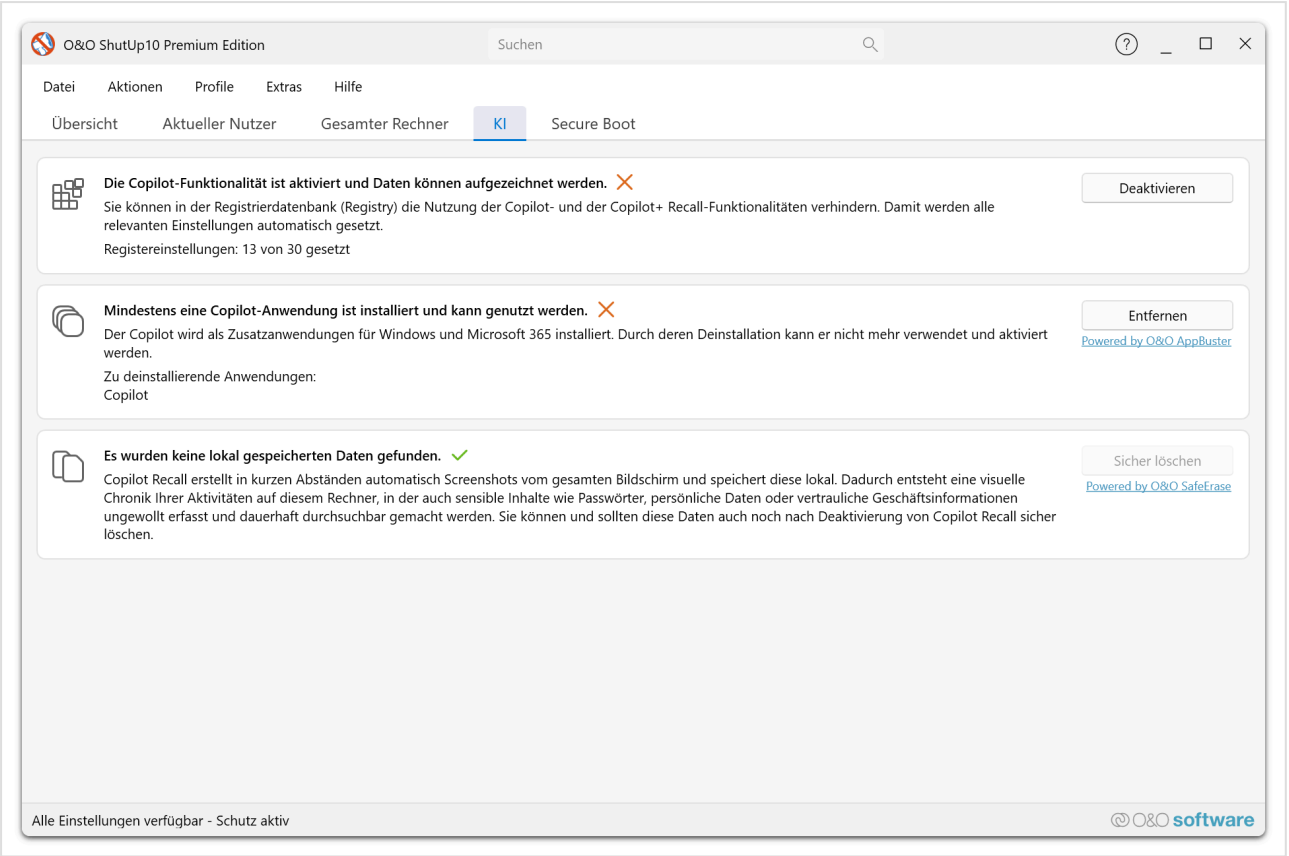
KI-Entfernung

Die KI-Entfernungsfunktion bietet einen umfassenden, dreistufigen Ansatz zur Entfernung von Microsoft Copilot und Recall-Komponenten von Ihrem System. Sie ist über die Registerkarte **KI** im Hauptfenster zugänglich und kombiniert die O&O ShutUp10-Einstellungs-Engine, die O&O AppBuster-Engine und die O&O SafeErase-Engine in einem einzigen Arbeitsablauf.

Free Edition:



Premium Edition:



Windows Copilot+ Recall erstellt automatisch Screenshots Ihrer Aktivitäten in regelmäßigen Abständen, speichert sie lokal und nutzt KI, um diesen Verlauf durchsuchbar zu machen. Die KI-Entfernungsfunktion ermöglicht es Ihnen, jede Ebene dieser Funktionalität zu adressieren: die Registry-Einstellungen, die sie aktivieren, die Anwendungen, die sie antreiben, und die Daten, die sie bereits auf Ihrem Gerät gespeichert hat.

KI-Einstellungen

Die erste Ebene steuert die Windows-Registry-Einstellungen, die Copilot und KI-Funktionalität regeln. Dies ist ein **Bündel der regulären O&O ShutUp10 Datenschutzeinstellungen** aus der Kategorie **Microsoft Copilot (in Windows)**, der Übersichtlichkeit halber zusammengefasst.

Was die Einstellungen steuern

Einstellung	Wirkung
Windows Copilot deaktivieren	Deaktiviert den Copilot KI-Assistenten in Windows vollständig.
Recall-Aktivierung deaktivieren	Verhindert, dass Copilot+ Recall auf Ihrem Gerät aktiviert wird.
KI-Datenanalyse deaktivieren	Verhindert, dass Windows KI zur lokalen Analyse Ihrer Daten nutzt.
Copilot-Schaltfläche aus der Taskleiste entfernen	Entfernt die Copilot-Schaltfläche aus der Windows-Taskleiste.
Image Creator in Microsoft Paint deaktivieren	Deaktiviert die KI-gestützte Bilderzeugung in Paint.
Cocreator in Microsoft Paint deaktivieren	Deaktiviert die KI-gestützte Cocreator-Funktion in Paint.
KI-gestützte Bildfüllung in Microsoft Paint deaktivieren	Deaktiviert die KI-gestützte generative Füllung in Paint.

Funktionsweise

- Die KI-Registerkarte zeigt einen Status an, der angibt, wie viele KI-bezogene Einstellungen derzeit deaktiviert sind (z.B. „5 von 8 deaktiviert").
- Klicken Sie auf **Deaktivieren**, um alle empfohlenen KI-Einstellungen auf einmal anzuwenden.
- Diese Einstellungen ändern die Windows-Registry auf die gleiche Weise wie das einzelne Umschalten in der Haupteinstellungsliste.

Da es sich um Standard-O&O ShutUp10-Registry-Einstellungen handelt, können sie **jederzeit wieder aktiviert** werden — entweder durch das individuelle Zurückschalten in der Haupteinstellungsliste oder durch erneutes Ausführen der KI-Einstellungen mit der entgegengesetzten Konfiguration.

> **Tip**
>
> Wenn Sie nur Copilot und Recall deaktivieren möchten, ohne Anwendungen oder Daten zu entfernen, reicht das alleinige Anwenden der KI-Einstellungen aus und ist vollständig reversibel.

KI-App-Entfernung (O&O AppBuster)

Die zweite Ebene entfernt Copilot-bezogene Anwendungen von Ihrem System mithilfe der **O&O AppBuster-Engine**. Diese erkennt und deinstalliert Microsoft Copilot+-Anwendungen, die als Windows Store-Apps installiert sind.

Was sie tut

- Scannt Ihr System nach installierten Copilot+-Anwendungen (sowohl benutzerspezifische als auch maschinenweite Installationen).
- Zeigt die Namen aller erkannten Copilot-Anwendungen an.
- Entfernt die Anwendungen, wenn Sie auf **Entfernen** klicken.

Erkennung

Die KI-Registerkarte zeigt den aktuellen Status an:

Status	Bedeutung
Anwendungen namentlich aufgelistet	Eine oder mehrere Copilot+-Apps sind auf Ihrem System installiert.
„Keine Copilot-Anwendungen gefunden"	Derzeit sind keine Copilot+-Apps installiert.

> **Danger**
>
> **Warnung — Diese Aktion kann von der Anwendung nicht rückgängig gemacht werden**
>
> Die Entfernung von Copilot+-Anwendungen ist eine **dauerhafte, unumkehrbare Operation** innerhalb von O&O ShutUp10. Sobald die Anwendungen deinstalliert sind, können sie nicht von dieser Anwendung neu installiert werden. Um sie wiederherzustellen, müssen Sie sie manuell über den Microsoft Store oder durch Zurücksetzen von Windows-Komponenten neu installieren.

Sichere Löschung von Recall-Daten (O&O SafeErase)

Die dritte Ebene löscht die Daten, die Copilot+ Recall bereits auf Ihrem Gerät gespeichert hat, sicher mithilfe der **O&O SafeErase-Engine**.

Was im Recall-Ordner gespeichert ist

Windows Copilot+ Recall speichert seine Daten im Ordner `CoreAIPlatform.00` innerhalb Ihres lokalen Anwendungsdatenverzeichnisses (`%LOCALAPPDATA%\CoreAIPlatform.00`). Dieser Ordner enthält:

- **Screenshots** — Periodische Aufnahmen Ihrer Bildschirmaktivität in regelmäßigen Abständen.
- **OCR-Textdaten** — Extrahierter Text aus den aufgenommenen Screenshots, der verwendet wird, um Ihre Aktivität durchsuchbar zu machen.
- **Index-Datenbanken** — Suchindizes, die es Recall ermöglichen, vergangene Aktivitäten zu finden und anzuzeigen.
- **KI-Modelldaten** — Lokale KI-Verarbeitungsartefakte für die Analyse auf dem Gerät.

Diese Daten können hochsensible Informationen enthalten: auf dem Bildschirm sichtbare Passwörter, private Nachrichten, Finanzdaten, persönliche Dokumente und alles andere, was auf Ihrem Bildschirm angezeigt wurde, während Recall aktiv war.

Funktionsweise

- Die KI-Registerkarte scannt den Recall-Datenordner und meldet die Anzahl der gefundenen Dateien und Verzeichnisse zusammen mit ihrer Gesamtgröße.
- Wenn keine Recall-Daten vorhanden sind, zeigt der Status **„Keine lokal gespeicherten Daten gefunden."**
- Klicken Sie auf **Vollständig entfernen**, um alle erkannten Recall-Daten sicher zu löschen.

Die sichere Löschung verwendet die O&O SafeErase-Engine, die Dateiinhalte vor dem Löschen überschreibt und sicherstellt, dass die Daten nicht mit Dateiwiederherstellungstools wiederhergestellt werden können.

Danger

Warnung — Diese Aktion kann in keiner Weise rückgängig gemacht werden

Die sichere Löschung mit O&O SafeErase ist **dauerhaft und irreversibel**. Im Gegensatz zur Standard-Dateilöschung (bei der Daten auf der Festplatte möglicherweise wiederherstellbar bleiben) überschreibt die sichere Löschung die Dateiinhalte mit Zufallsdaten, bevor sie entfernt werden. Sobald die Recall-Daten sicher gelöscht sind, können sie mit keinem Mittel wiederhergestellt werden — nicht von O&O ShutUp10, nicht von Windows und nicht von einem Datenwiederherstellungstool.

Fahren Sie nur fort, wenn Sie sicher sind, dass Sie keine der von Recall gespeicherten Daten mehr benötigen.

Vollständige KI-Entfernung

Für maximalen Schutz können Sie alle drei Ebenen in einem einzigen Vorgang zusammen ausführen. Wenn Sie sich entscheiden, alle Komponenten zu deaktivieren, fragt ein Bestätigungsdialog:

> „Sind Sie sicher, dass Sie alle Komponenten deaktivieren möchten?"

Die Bestätigung wird:

1. Alle KI-bezogenen Registry-Einstellungen **deaktivieren** (reversibel).
2. Alle erkannten Copilot+-Anwendungen **entfernen** (nicht von der Anwendung reversibel).
3. Alle auf dem Gerät gespeicherten Recall-Daten **sicher löschen** (dauerhaft irreversibel).

Statusübersicht

Die Premium Edition-Übersichtsregisterkarte enthält einen KI-Statusindikator, der eine schnelle Zusammenfassung Ihres Copilot+-Entfernungsstatus bietet:

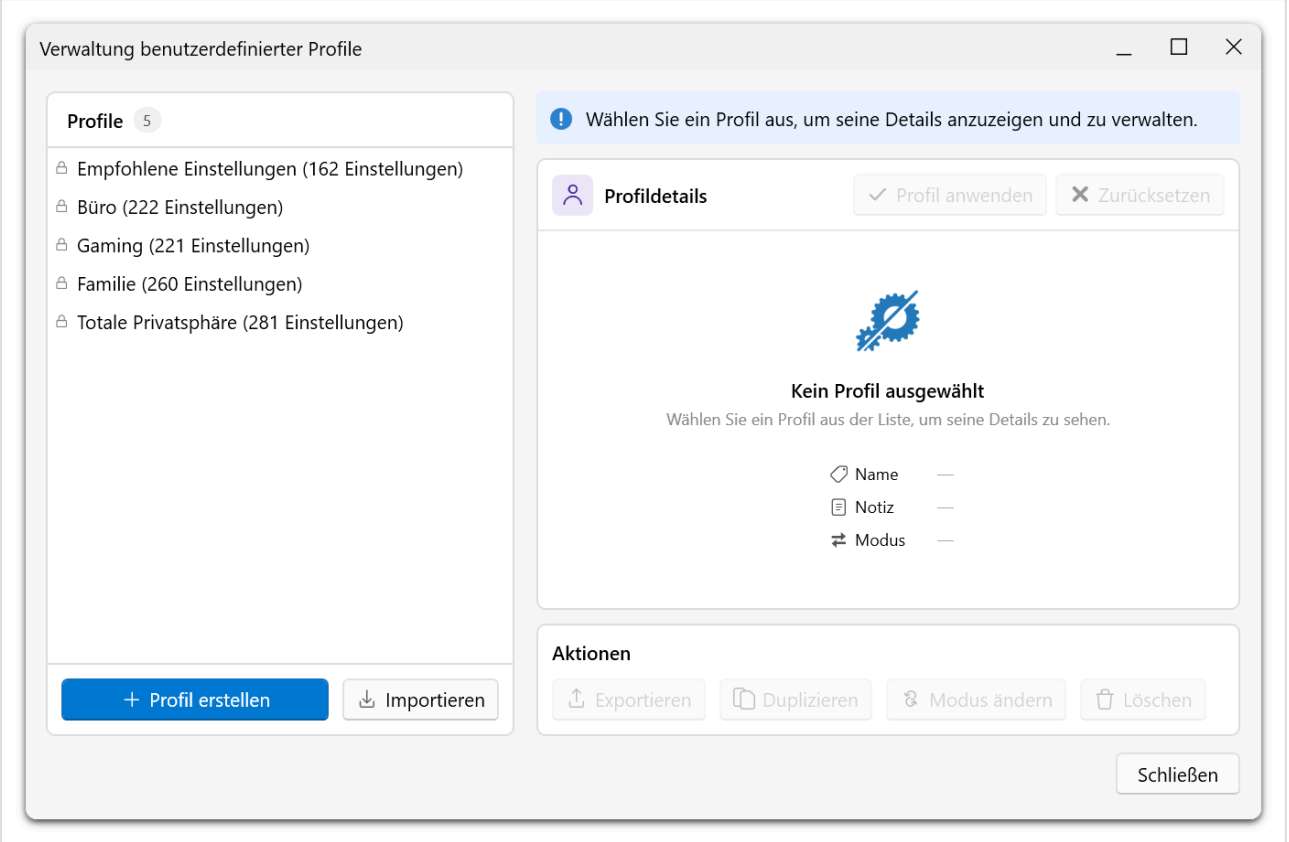
Komponente	Statuswerte
Einstellungen	„X von Y deaktiviert"
Anwendungen	„Nicht installiert" oder „X installiert"
Recall-Dateien	„Keine Dateien erkannt" oder „Dateien erkannt"

Der Gesamtstatus wird angezeigt als:

Gesamtstatus	Bedeutung
Alle Copilot+-Komponenten entfernt	Alle Einstellungen deaktiviert, keine Apps installiert, keine Recall-Dateien.
Teilweise entfernt	Einige Komponenten wurden adressiert, aber nicht alle.
Copilot+-Komponenten aktiv	Es wurden keine Entfernungsaktionen durchgeführt.

Profile & Export

O&O ShutUp10 unterstützt das Speichern und Laden von Datenschutzeinstellungsprofilen. Diese Funktion ist in der Free und Premium Edition verfügbar, mit zusätzlichen Möglichkeiten in der Premium Edition.



Überblick

Profile ermöglichen es Ihnen, Ihre aktuelle Datenschutzkonfiguration zu speichern und später erneut anzuwenden. Dies ist nützlich für die Aufrechterhaltung konsistenter Einstellungen über Neuinstallationen hinweg, das Teilen von Konfigurationen oder das Wechseln zwischen verschiedenen Datenschutzstufen.

Funktionen

Profile speichern

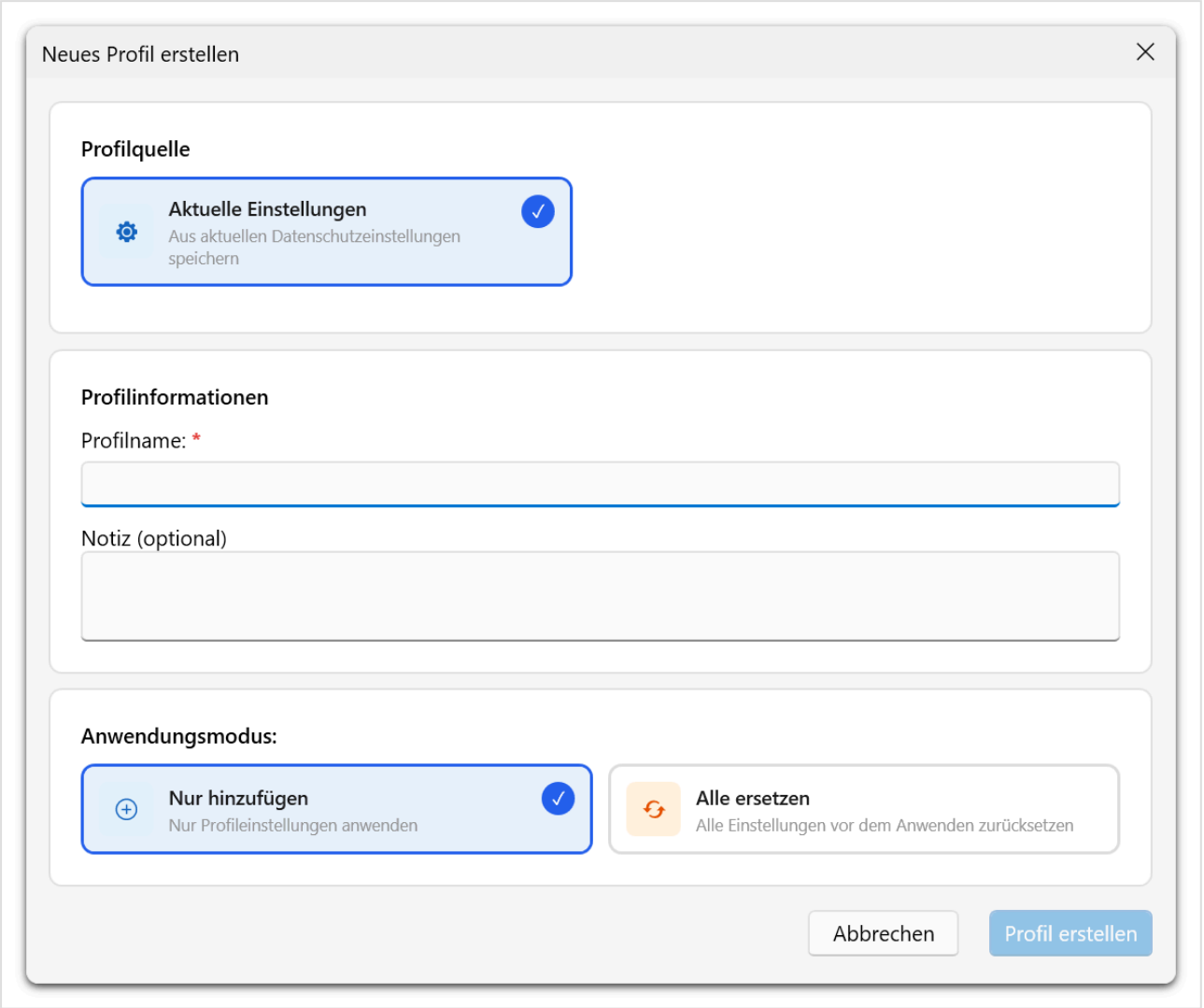
Speichern Sie Ihren aktuellen Satz von Datenschutzeinstellungen als benanntes Profil. Sie können mehrere Profile für verschiedene Szenarien erstellen (z.B. ein strenges Datenschutzprofil und ein ausgewogenes Profil).

Profile laden

Laden Sie ein zuvor gespeichertes Profil, um dessen Datenschutzeinstellungen sofort anzuwenden. Dies ist besonders nützlich nach einer frischen Windows-Installation oder einem größeren Windows-Update.

Exportieren und Importieren

Exportieren Sie Ihre Datenschutzkonfiguration als Datei, die mit anderen geteilt oder auf einen anderen Rechner übertragen werden kann. Importieren Sie eine Konfigurationsdatei, um die Datenschutzeinstellungen einer anderen Person anzuwenden.



Befehlszeilenunterstützung

O&O ShutUp10 unterstützt Befehlszeilenparameter zum Anwenden von Profilen, was Automatisierung und Integration mit Bereitstellungsskripten ermöglicht.

Tip

Speichern Sie ein Profil Ihrer bevorzugten Einstellungen vor jedem größeren Windows-Update. Wenn das Update Ihre Datenschutzeinstellungen zurücksetzt, können Sie sie schnell wiederherstellen, indem Sie Ihr gespeichertes Profil laden.

Profildateistruktur

O&O ShutUp10++ speichert Profile als Konfigurationsdateien, die alle Ihre gespeicherten Datenschutzeinstellungen enthalten. Diese Seite erklärt, wie Profildateien aufgebaut sind und was jedes Attribut bedeutet, damit Sie Ihre exportierten Profile verstehen, überprüfen oder manuell bearbeiten können.

Dateiformat

Profildateien verwenden das **INI-Format** — ein einfaches textbasiertes Format mit Abschnitten und Schlüssel-Wert-Paaren. Sie können sie mit jedem Texteditor (z.B. Notepad) öffnen und überprüfen.

Eine Profildatei besteht aus zwei Abschnitten: `[Profile]` (Metadaten über das Profil) und `[Settings]` (die eigentlichen Datenschutzeinstellungen).

Beispiel-Profildatei

```
[Profile]
Id=a3f8b2c1-4d5e-6f7a-8b9c-0d1e2f3a4b5c
Name=Mein Datenschutzprofil
Description=Ausgewogene Datenschutzeinstellungen für den täglichen Gebrauch
Created=2025-03-15T10:30:00Z
Modified=2025-04-01T14:22:00Z
IsSystem=false
Icon=custom

[Settings]
DisableTelemetry=true
DisableAdvertisingId=true
DisableLocationTracking=true
DisableWebSearch=false
DisableCortana=false
```

Profilattribute

Abschnitt `[Profile]`

Der Abschnitt `[Profile]` enthält Metadaten, die das Profil identifizieren und beschreiben.

Attribut	Beschreibung	Beispiel
Id	Ein eindeutiger Bezeichner (GUID) für das Profil. Wird automatisch bei der Erstellung generiert.	`a3f8b2c1-4d5e-6f7a-8b9c-0d1e2f3a4b5c`
Name	Der Anzeigename des Profils. Muss unter allen Profilen eindeutig sein.	`Mein Datenschutzprofil`
Description	Eine optionale Notiz oder Beschreibung, die den Zweck des Profils erklärt.	`Ausgewogene Datenschutzeinstellungen für den täglichen Gebrauch`
Created	Datum und Uhrzeit der Profilerstellung (ISO 8601-Format).	`2025-03-15T10:30:00Z`
Modified	Datum und Uhrzeit der letzten Änderung (ISO 8601-Format).	`2025-04-01T14:22:00Z`
IsSystem	Gibt an, ob es sich um ein eingebautes Systemprofil (`true`) oder ein benutzererstelltes Profil (`false`) handelt.	`false`
Icon	Das dem Profil zugeordnete Symbol in der Anwendungsoberfläche.	`custom`

Abschnitt `[Settings]`

Der Abschnitt `[Settings]` enthält die eigentlichen Datenschutzeinstellungen als Schlüssel-Wert-Paare. Jeder Eintrag repräsentiert eine Datenschutzeinstellung, die von O&O ShutUp10++ gesteuert wird.

Komponente	Beschreibung	Beispiel
Schlüssel	Der interne Name der Datenschutzeinstellung.	`DisableTelemetry`
Wert	Der gewünschte Status für diese Einstellung (`true` = Datenschutz aktiviert, `false` = Windows-Standard).	`true`

Die Einstellungen entsprechen denselben Optionen, die Sie in der O&O ShutUp10++ Benutzeroberfläche sehen. Nur Einstellungen, die explizit konfiguriert sind, werden in der Datei aufgeführt — nicht aufgelistete Einstellungen bleiben beim Anwenden des Profils unverändert.

Profiltypen

Eingebaute (System-)Profile

Diese Profile werden von O&O ShutUp10++ bereitgestellt und sind immer verfügbar:

- Können nicht geändert oder gelöscht werden
- Werden automatisch mit Anwendungsupdates aktualisiert
- Wenden Einstellungen immer im **Nur-Hinzufügen**-Modus an (ändern nur Einstellungen, die noch nicht konfiguriert sind)
- Gekennzeichnet durch `IsSystem=true` in der Datei

Benutzererstellte (Benutzerdefinierte) Profile

Dies sind Profile, die Sie selbst erstellen:

- Können erstellt, umbenannt, bearbeitet, gelöscht, exportiert und importiert werden
- Können entweder den **Nur-Hinzufügen**- oder den **Alles-Ersetzen**-Anwendungsmodus verwenden
- Gekennzeichnet durch `IsSystem=false` in der Datei
- Werden zusammen mit Ihren Benutzereinstellungen gespeichert

Anwendungsmodi

Beim Anwenden eines Profils unterstützt O&O ShutUp10++ zwei Modi:

Modus	Verhalten
Nur-Hinzufügen	Wendet nur Einstellungen aus dem Profil an, die nicht mit Ihrer aktuellen Konfiguration in Konflikt stehen. Vorhandene Einstellungen werden nicht überschrieben.
Alles-Ersetzen	Überschreibt alle aktuellen Einstellungen mit den im Profil definierten Werten. Nicht im Profil enthaltene Einstellungen werden auf Windows-Standards zurückgesetzt.

Eingebaute Profile verwenden immer den Nur-Hinzufügen-Modus. Bei benutzerdefinierten Profilen können Sie beim Anwenden wählen, welcher Modus verwendet werden soll.

Profile exportieren und teilen

Wenn Sie ein Profil exportieren, enthält die resultierende Datei die vollständigen Abschnitte `[Profile]` und `[Settings]` wie oben beschrieben. Sie können:

- Die Datei mit anderen Benutzern oder Rechnern teilen
- Profile vor einem Windows-Update sichern
- Die Datei manuell bearbeiten, um Einstellungen vor dem Import anzupassen

> **Tip**
>
> Öffnen Sie nach dem Export eines Profils die Datei in einem Texteditor, um genau zu überprüfen, welche Einstellungen enthalten sind und auf welche Werte sie gesetzt sind.

FAQ

- **Kann ich eine Profildatei manuell bearbeiten?** Ja, Profildateien sind reiner Text. Sie können sie in jedem Texteditor öffnen, um Einstellungen vor dem Import zu überprüfen oder zu ändern.
- **Was passiert, wenn ich die Id ändere?** Die Anwendung verwendet die Id zur Identifikation von Profilen. Eine Änderung führt dazu, dass die Datei beim Import als neues Profil behandelt wird.
- **Müssen Profilnamen eindeutig sein?** Ja. Wenn Sie ein Profil mit einem bereits vorhandenen Namen importieren, werden Sie aufgefordert, es umzubenennen.
- **Was passiert mit Einstellungen, die nicht im Profil aufgelistet sind?** Sie bleiben im Nur-Hinzufügen-Modus unverändert oder werden im Alles-Ersetzen-Modus auf Windows-Standards zurückgesetzt.
- **Sind Profile zwischen Rechnern portabel?** Ja. Sie können ein Profil von einem Rechner exportieren und auf einem anderen mit O&O ShutUp10++ importieren.

Bearbeitungsmodus

Der Bearbeitungsmodus bietet eine sichere Möglichkeit, mehrere Datenschutzeinstellungsänderungen in der Vorschau zu betrachten und zu bündeln, bevor sie auf Ihr System angewendet werden. Er ist in der Free und Premium Edition verfügbar.

Motivation

Standardmäßig wird das Umschalten einer Datenschutzeinstellung in O&O ShutUp10 sofort in der Windows-Registry angewendet. Das ist zwar praktisch für einzelne Anpassungen, kann aber riskant sein, wenn viele Änderungen auf einmal vorgenommen werden — besonders wenn eine bestimmte Kombination von Einstellungen unerwartetes Verhalten verursacht.

Der Bearbeitungsmodus löst dies, indem er alle Änderungen **puffert**, anstatt sie sofort anzuwenden. Sie können Ihre beabsichtigten Änderungen überprüfen, alle auf einmal anwenden, sie als benutzerdefiniertes Profil speichern (nur Premium) oder vollständig verwerfen. Dies macht den Bearbeitungsmodus zur sichersten Methode, mit Datenschutzkonfigurationen zu experimentieren.

Funktionsweise

Bearbeitungsmodus aktivieren

1. Öffnen Sie das **Bearbeiten**-Menü im Hauptfenster.
2. Klicken Sie auf **Bearbeitungsmodus aktivieren**.

Wenn der Bearbeitungsmodus aktiv ist:

- Ein Benachrichtigungsbanner erscheint oben in der Einstellungsliste und zeigt an, dass der Bearbeitungsmodus aktiv ist und Änderungen gepuffert werden.
- Das Banner zeigt die Anzahl der gepufferten Änderungen an (z.B. „5 gepuffert").
- Einstellungen, die Sie umschalten, werden hervorgehoben, aber **noch nicht** auf das System angewendet.

Änderungen vornehmen

Während der Bearbeitungsmodus aktiv ist, schalten Sie Datenschutzeinstellungen wie gewohnt um. Jede Änderung wird in einem Puffer gespeichert, anstatt in die Registry geschrieben zu werden. Sie können Einstellungen frei ein- und ausschalten, ohne sofortige Auswirkungen auf das System.

Gepufferte Änderungen anwenden

Wenn Sie mit Ihren Änderungen zufrieden sind:

1. Öffnen Sie das **Bearbeiten**-Menü und klicken Sie auf **Anwenden**, oder klicken Sie auf die Schaltfläche **Anwenden** im Bearbeitungsmodus-Banner.
2. Ein Bestätigungsdialog zeigt die Anzahl der gepufferten Änderungen und bittet um Bestätigung.
3. Alle gepufferten Änderungen werden auf einmal auf das System angewendet.

Gepufferte Änderungen verwerfen

Wenn Sie alle gepufferten Änderungen verwerfen möchten, ohne sie anzuwenden:

1. Öffnen Sie das **Bearbeiten**-Menü und klicken Sie auf **Verwerfen**, oder klicken Sie auf die Schaltfläche **Verwerfen** im Bearbeitungsmodus-Banner.
2. Ein Bestätigungsdialog fragt, ob Sie das Verwerfen der Änderungen bestätigen möchten.
3. Alle gepufferten Änderungen werden entfernt und die Einstellungen kehren zu ihrem vorherigen Zustand zurück.

Bearbeitungsmodus deaktivieren

Wenn Sie den Bearbeitungsmodus deaktivieren (indem Sie erneut auf **Bearbeitungsmodus aktivieren** klicken, um ihn umzuschalten), prüft die Anwendung auf nicht angewendete gepufferte Änderungen. Wenn ausstehende Änderungen vorhanden sind, werden Sie aufgefordert, sie entweder anzuwenden oder zu verwerfen, bevor der Bearbeitungsmodus deaktiviert wird.

Änderungen als Profil speichern Premium

In der Premium Edition können Sie Ihre gepufferten Änderungen als wiederverwendbares benutzerdefiniertes Profil speichern:

1. Aktivieren Sie den Bearbeitungsmodus und konfigurieren Sie Ihre gewünschten Einstellungen.
2. Öffnen Sie das **Bearbeiten**-Menü und klicken Sie auf **Benutzerdefiniertes Profil speichern**.
3. Geben Sie einen Profilnamen und eine optionale Beschreibung ein.
4. Die gepufferten Änderungen werden als benanntes Profil gespeichert, das später über den Profil-Editor erneut angewendet werden kann.

Dieser Arbeitsablauf ist der primäre Weg zur Erstellung benutzerdefinierter Profile — er stellt sicher, dass nur Ihre beabsichtigten Änderungen im Profil erfasst werden.

Vorteile des Bearbeitungsmodus

Vorteil	Beschreibung
Sicherheit	Keine Änderungen werden angewendet, bis Sie ausdrücklich bestätigen, was das Risiko unbeabsichtigter Systemänderungen reduziert.
Stapeloperationen	Wenden Sie mehrere zusammenhängende Änderungen gleichzeitig an, anstatt eine nach der anderen.
Vorschau vor dem Festlegen	Überprüfen Sie den vollständigen Satz beabsichtigter Änderungen, bevor eine wirksam wird.
Einfaches Rückgängigmachen	Verwerfen Sie alle gepufferten Änderungen mit einer einzigen Aktion, wenn Sie Ihre Meinung ändern.
Profilerstellung	Speichern Sie Ihren kuratierten Satz von Änderungen als wiederverwendbares Profil (nur Premium).

> **Tip**
>
> Verwenden Sie den Bearbeitungsmodus, wenn Sie planen, mehr als ein paar Einstellungen auf einmal zu ändern. Er bietet ein Sicherheitsnetz, das versehentliche Änderungen verhindert und es Ihnen ermöglicht, die vollständigen Auswirkungen Ihrer Änderungen zu überprüfen, bevor Sie sie festlegen.

Einstellungsdialog

Der Einstellungsdialog zentralisiert alle Anwendungskonfigurationsoptionen in einer einzigen, registerkartenbasierten Oberfläche. Er ist über **Ansicht** → **Einstellungen…** im Hauptmenü erreichbar.

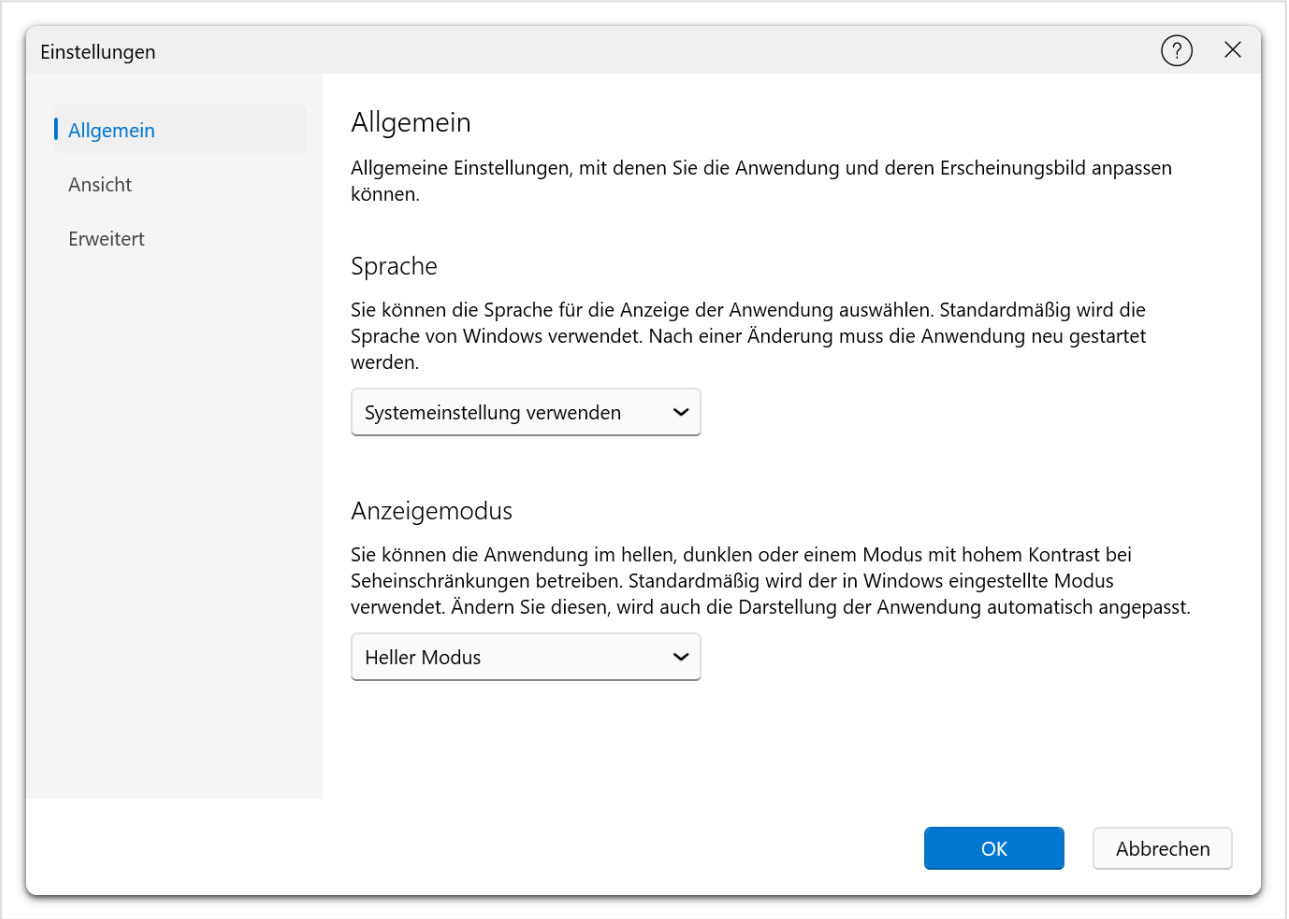
Überblick

Der Einstellungsdialog ersetzt die zuvor über verschiedene Menüs verteilten Konfigurationsoptionen. Alle Änderungen werden sofort gespeichert, wenn Sie auf **OK** klicken, und visuelle Änderungen (Design, Farbschema) werden in Echtzeit angewendet.

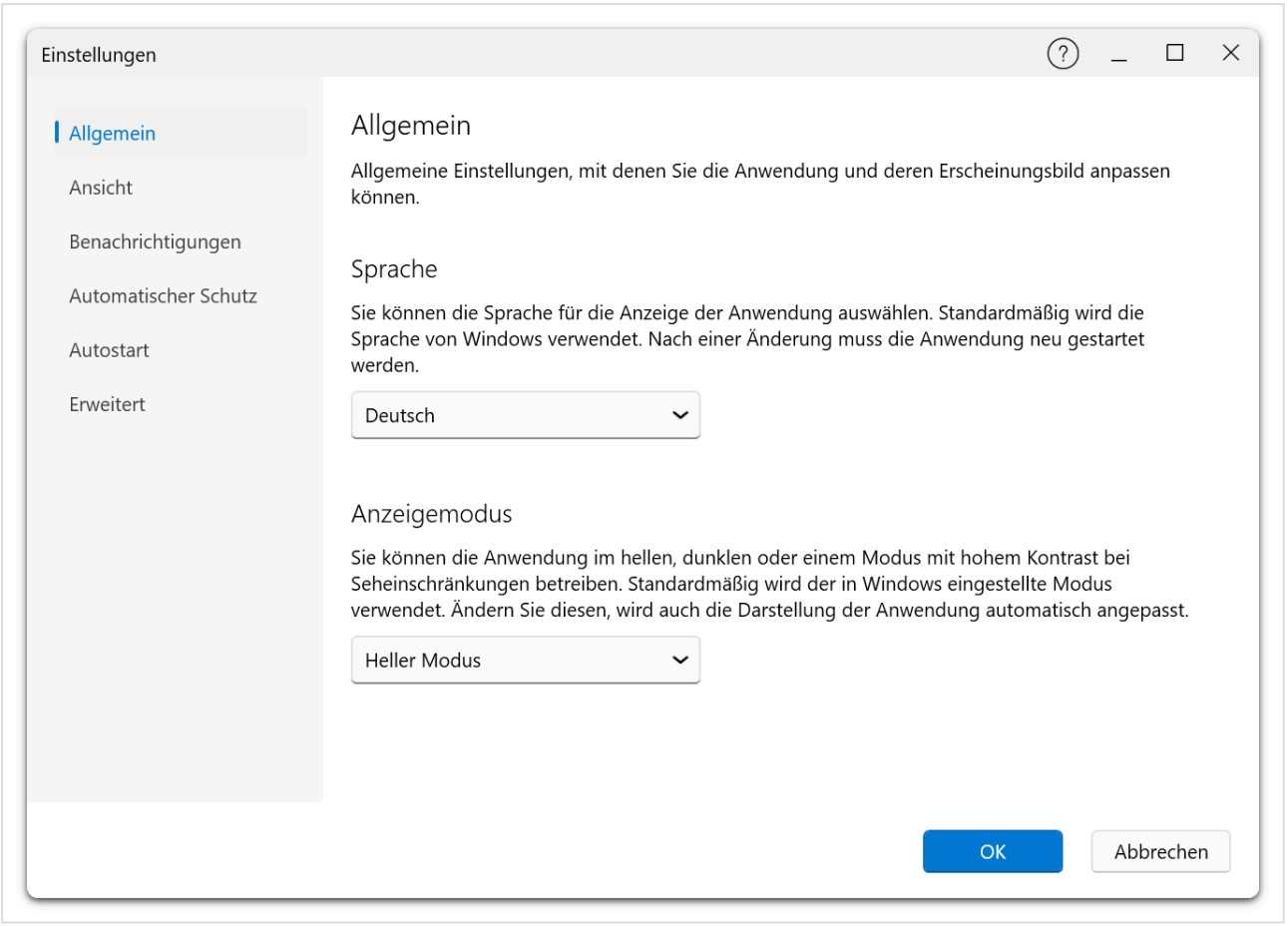
Registerkarte „Allgemein"

Allgemeine Einstellungen, mit denen Sie die Anwendung und ihr Erscheinungsbild anpassen können.

Free Edition:



Premium Edition:



Sprache

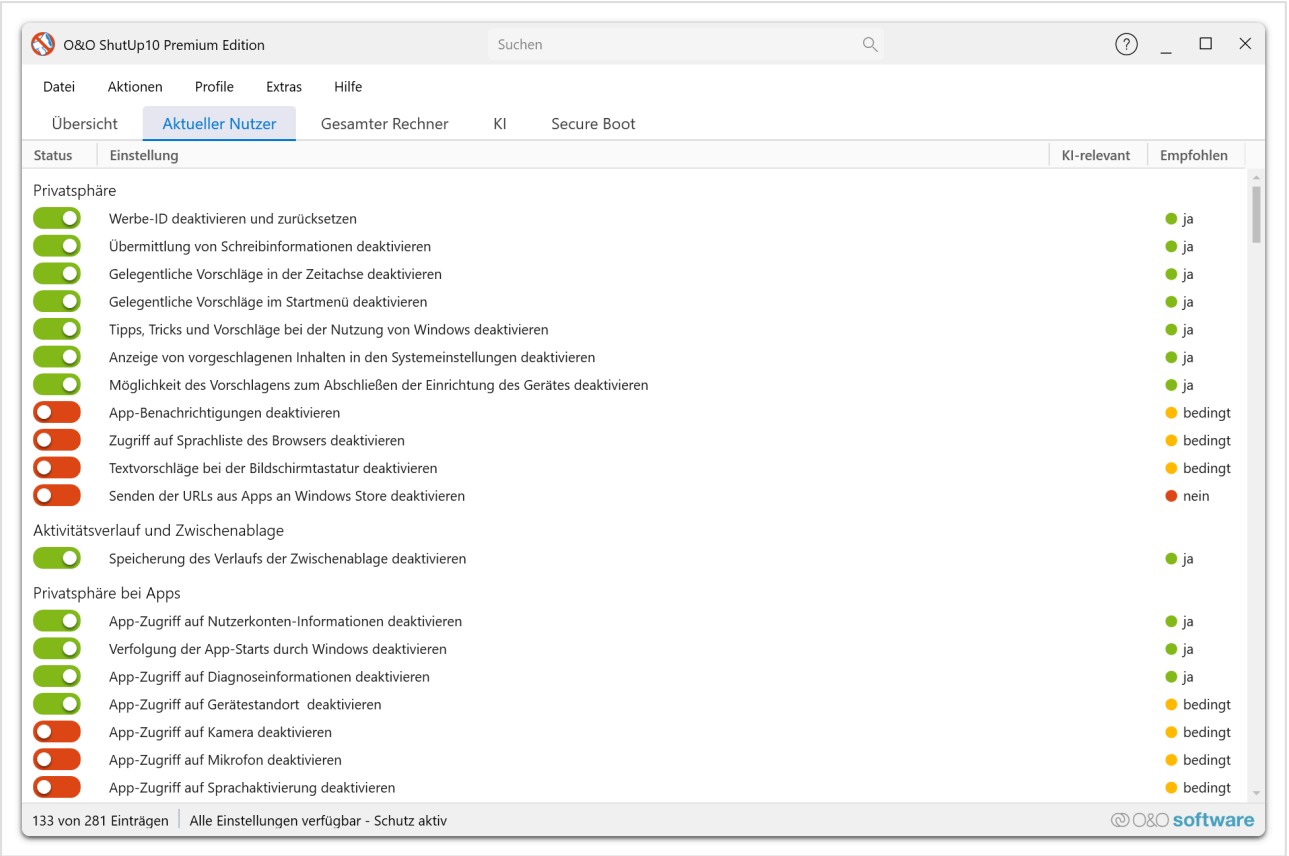
Wählen Sie die Anzeigesprache für die Anwendung. Verfügbare Sprachen umfassen Englisch (Standard), Deutsch, Spanisch, Französisch, Italienisch, Japanisch, Russisch und Chinesisch. Das Ändern der Sprache erfordert einen Neustart der Anwendung.

App-Ansichtsmodus

Wählen Sie das Anwendungsdesign:

Option	Beschreibung
System	Folgt dem aktuellen Windows-Design (hell oder dunkel).
Hell	Erzwingt ein helles Erscheinungsbild.
Dunkel	Erzwingt ein dunkles Erscheinungsbild.
Hoher Kontrast Schwarz	Hochkontrast-Design mit schwarzem Hintergrund für Barrierefreiheit.
Hoher Kontrast Weiß	Hochkontrast-Design mit weißem Hintergrund für Barrierefreiheit.

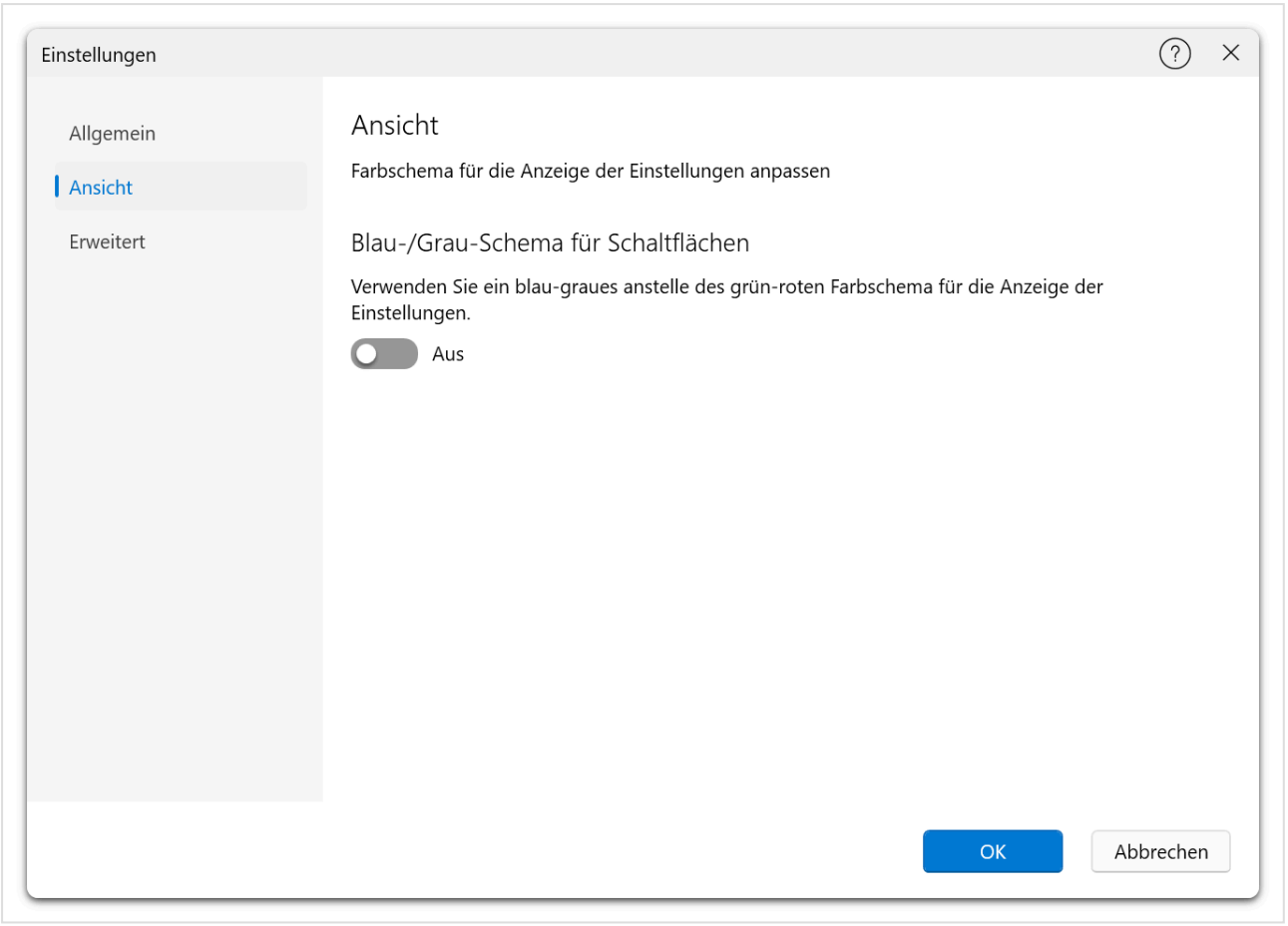
Designänderungen werden sofort ohne Neustart der Anwendung angewendet.



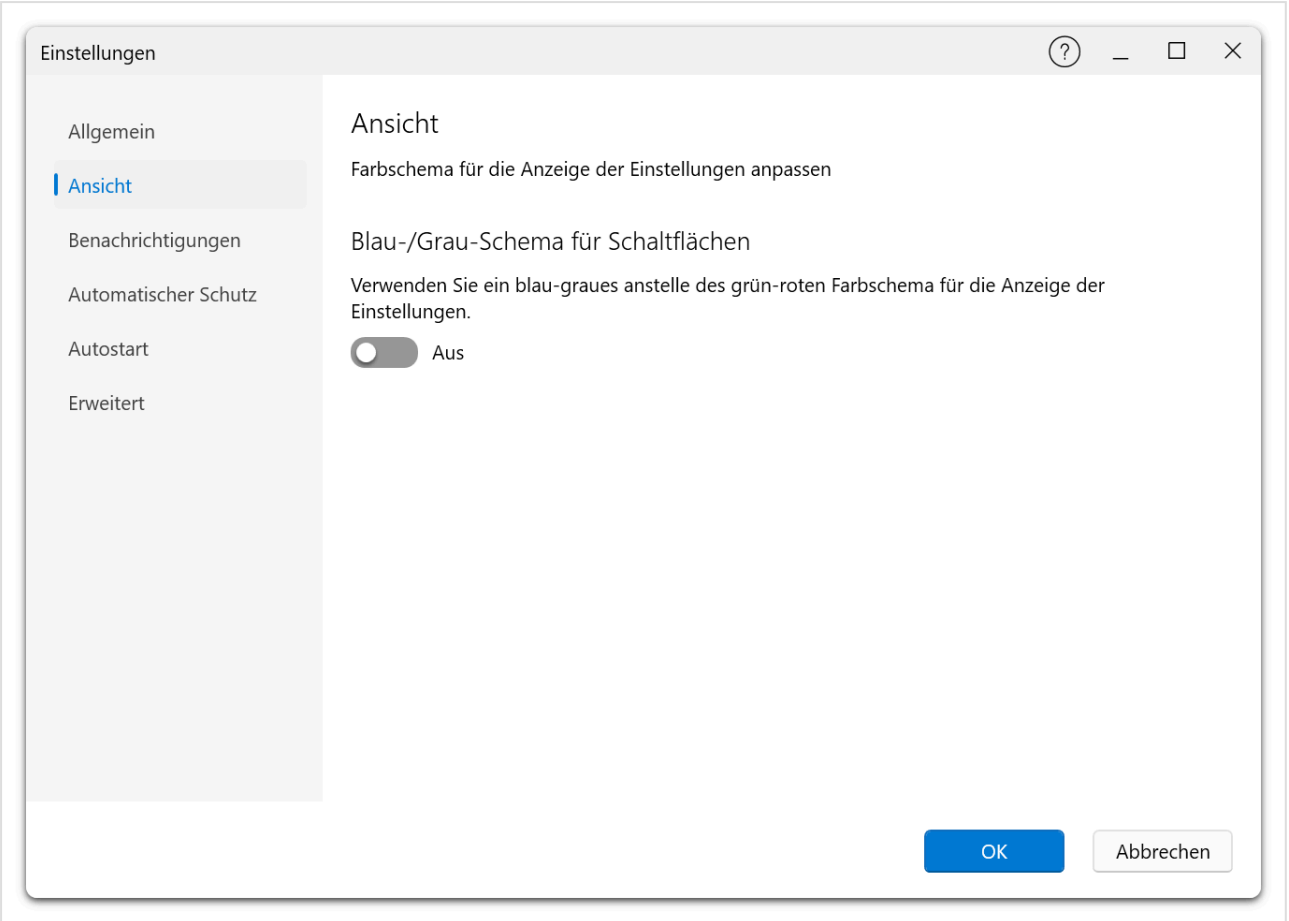
Registerkarte „Ansicht"

Passen Sie das Farbschema für die Anzeige der Einstellungen an.

Free Edition:



Premium Edition:



Blau/Graue Schaltflächen verwenden

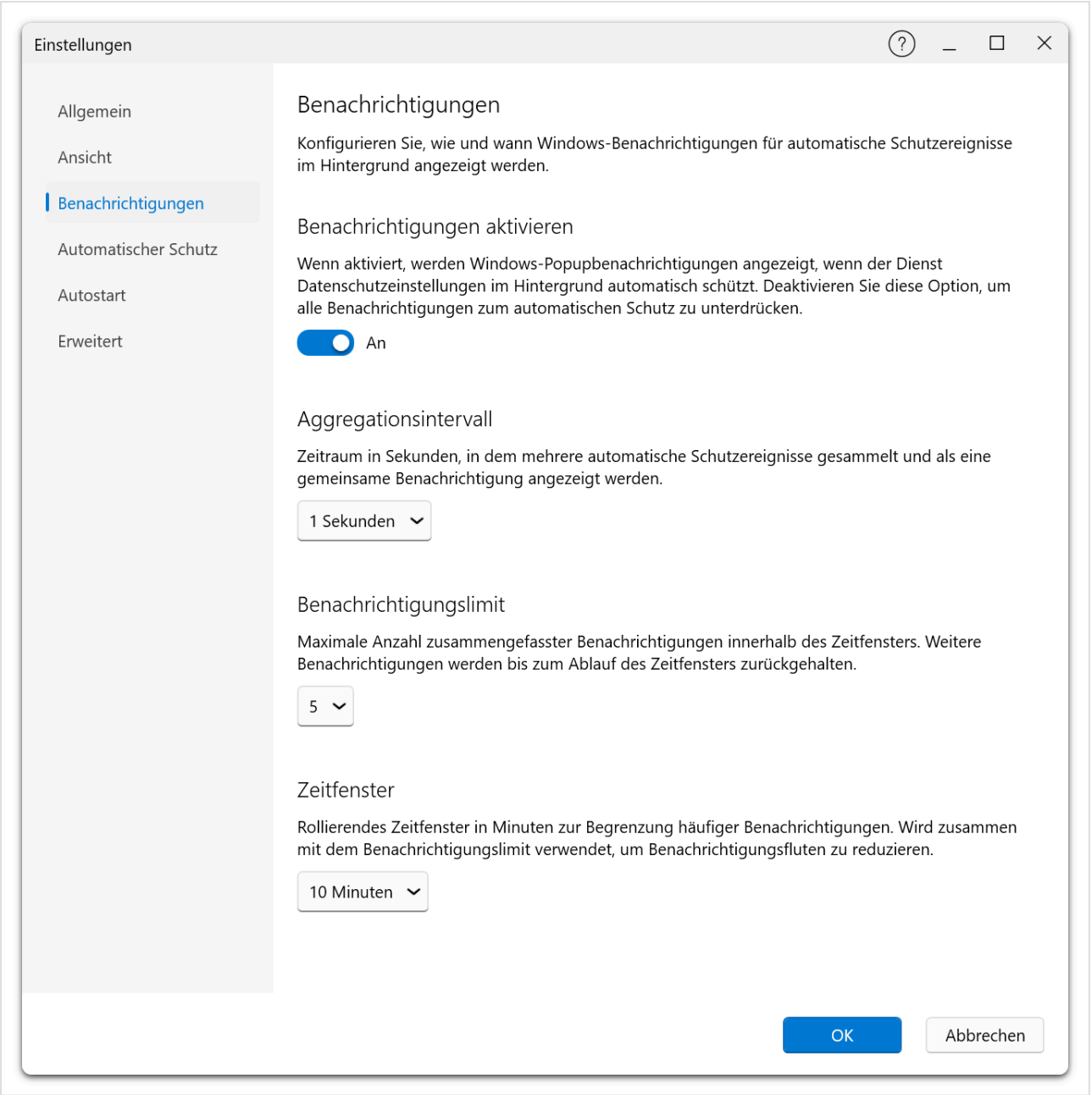
Wechseln Sie zwischen zwei Farbschemata für die Einstellungs-Umschalter:

- **Grün/Rot** (Standard) — Grün zeigt eine aktive (datenschutzschützende) Einstellung an; Rot zeigt eine inaktive Einstellung an.
- **Blau/Grau** — Ein neutrales Farbschema mit Blau- und Grautönen.

Die Farbschemaänderung wird in Echtzeit angewendet.

Registerkarte „Benachrichtigungen" Premium

Konfigurieren Sie, wie und wann Windows-Benachrichtigungen für automatische Schutzereignisse im Hintergrund angezeigt werden.



Diese Registerkarte ist nur in der Premium Edition verfügbar und erfordert, dass der Hintergrunddienst läuft. Wenn der Dienst nicht verfügbar ist, wird eine Warnmeldung angezeigt und die Steuerelemente sind deaktiviert.

Benachrichtigungen aktivieren

Wenn aktiviert, werden Windows-Toast-Benachrichtigungen angezeigt, wenn der Dienst automatisch Datenschutzeinstellungen im Hintergrund schützt. Deaktivieren Sie diese Option, um alle automatischen Schutzbenachrichtigungen zu unterdrücken.

Aggregationsintervall

Definiert, wie lange der Dienst (in Sekunden) wartet, bevor er eine zusammengefasste Benachrichtigung für mehrere Ereignisse sendet. Verfügbare Werte: 1, 2, 5, 10, 15, 30, 60 oder 120 Sekunden.

Unterdrückungsschwelle

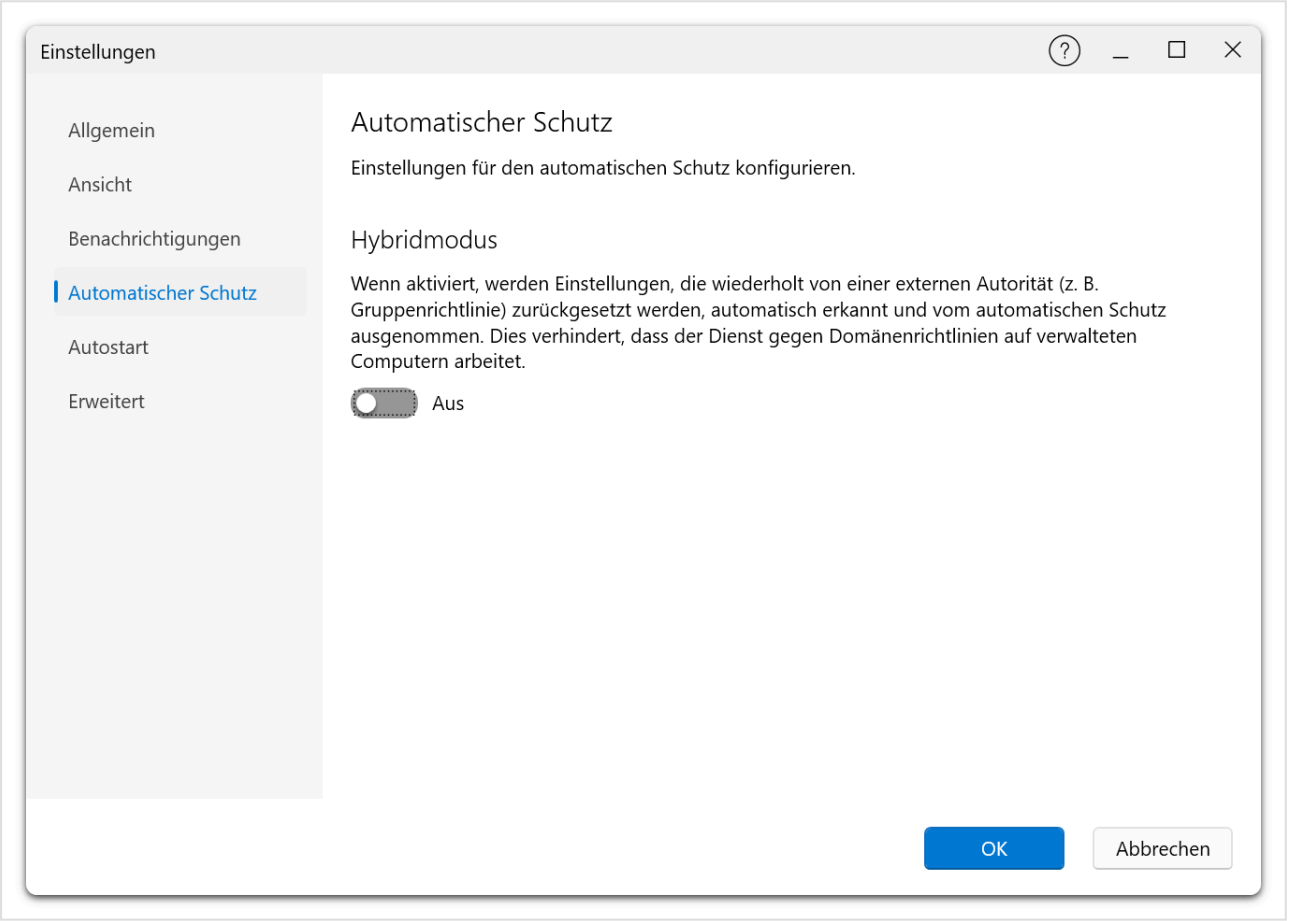
Maximale Anzahl von Benachrichtigungen, die innerhalb des Unterdrückungsfensters erlaubt sind, bevor weitere Benachrichtigungen unterdrückt werden. Verfügbare Werte: 1, 2, 3, 5, 10, 15 oder 20.

Unterdrückungsfenster

Rollendes Zeitfenster (in Minuten), das zusammen mit der Unterdrückungsschwelle zur Flutprävention verwendet wird. Verfügbare Werte: 1, 2, 5, 10, 15, 30 oder 60 Minuten.

Registerkarte „Automatischer Schutz" Premium

Konfigurieren Sie die Einstellungen für den automatischen Schutz.



Diese Registerkarte ist nur in der Premium Edition verfügbar und erfordert, dass der Hintergrunddienst läuft.

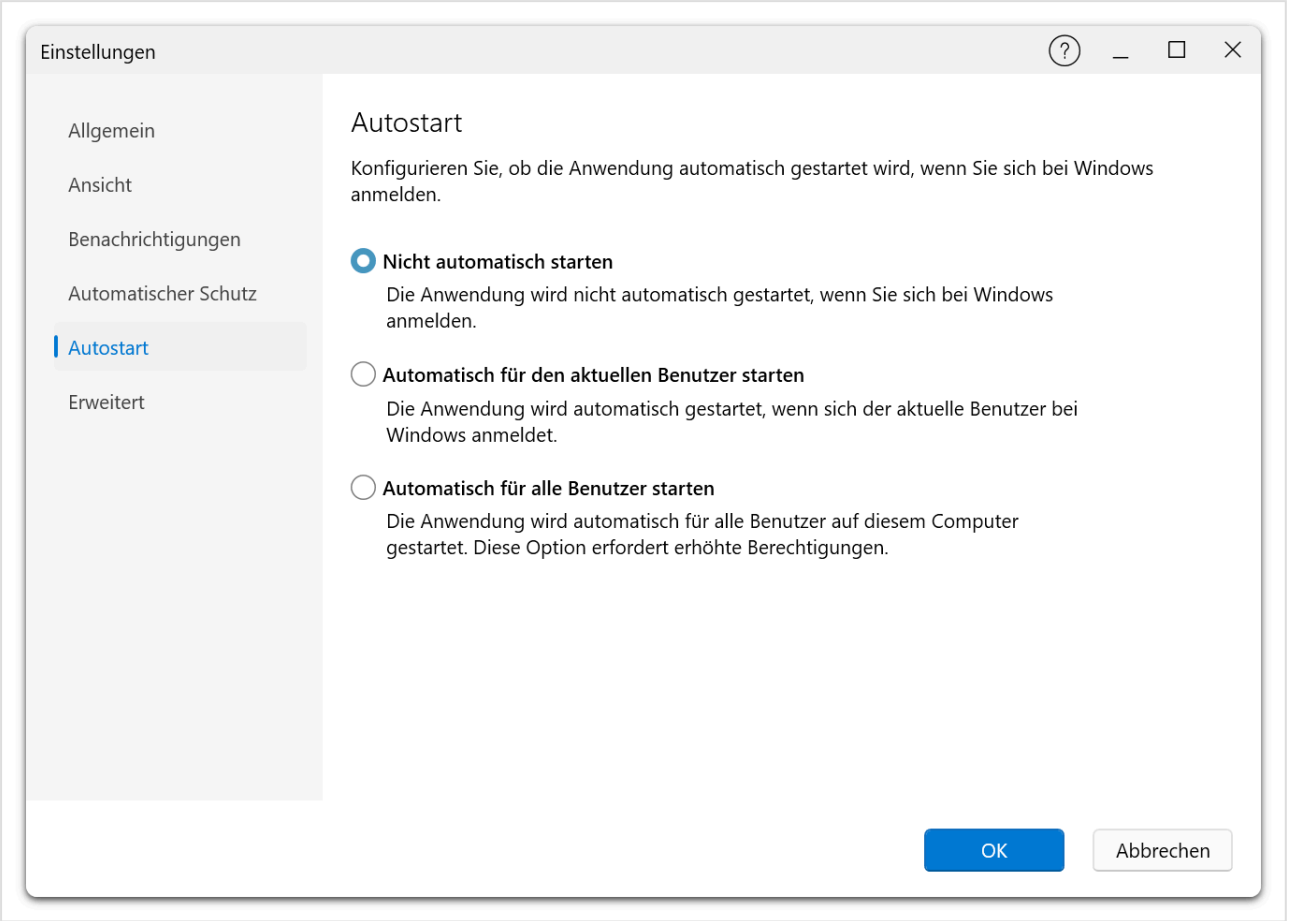
Hybrid-Modus

Wenn aktiviert, werden Einstellungen, die wiederholt von einer externen Autorität (z.B. Gruppenrichtlinie) zurückgesetzt werden, automatisch erkannt und vom automatischen Schutz ausgeschlossen. Dies verhindert, dass der Dienst auf verwalteten Rechnern gegen Domänenrichtlinien kämpft.

Der Hybrid-Modus ist besonders nützlich in Unternehmensumgebungen, in denen bestimmte Datenschutzeinstellungen durch organisatorische Gruppenrichtlinien gesteuert werden und nicht vom ShutUp10-Dienst überschrieben werden sollten.

Registerkarte „Autostart" Premium

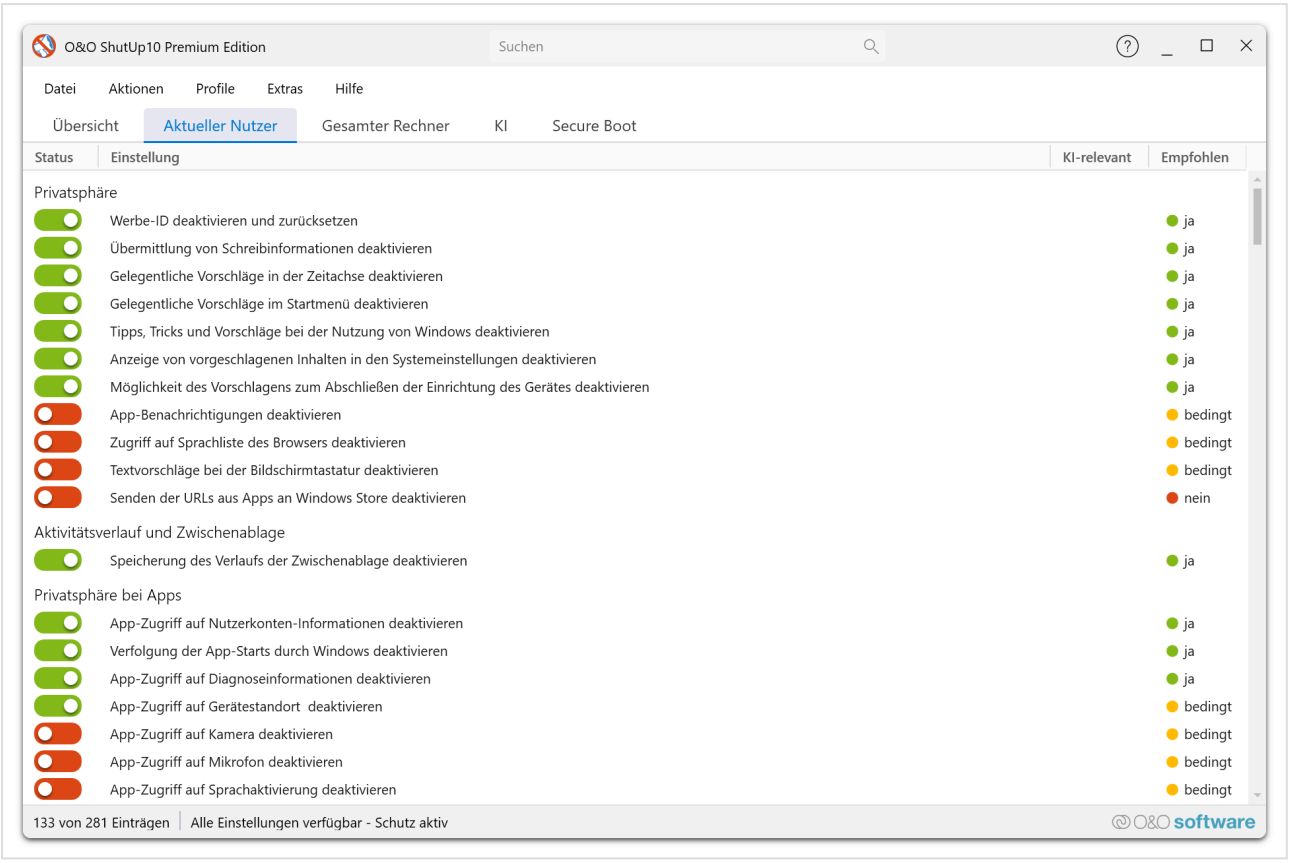
Konfigurieren Sie, ob die Anwendung automatisch startet, wenn Sie sich bei Windows anmelden.

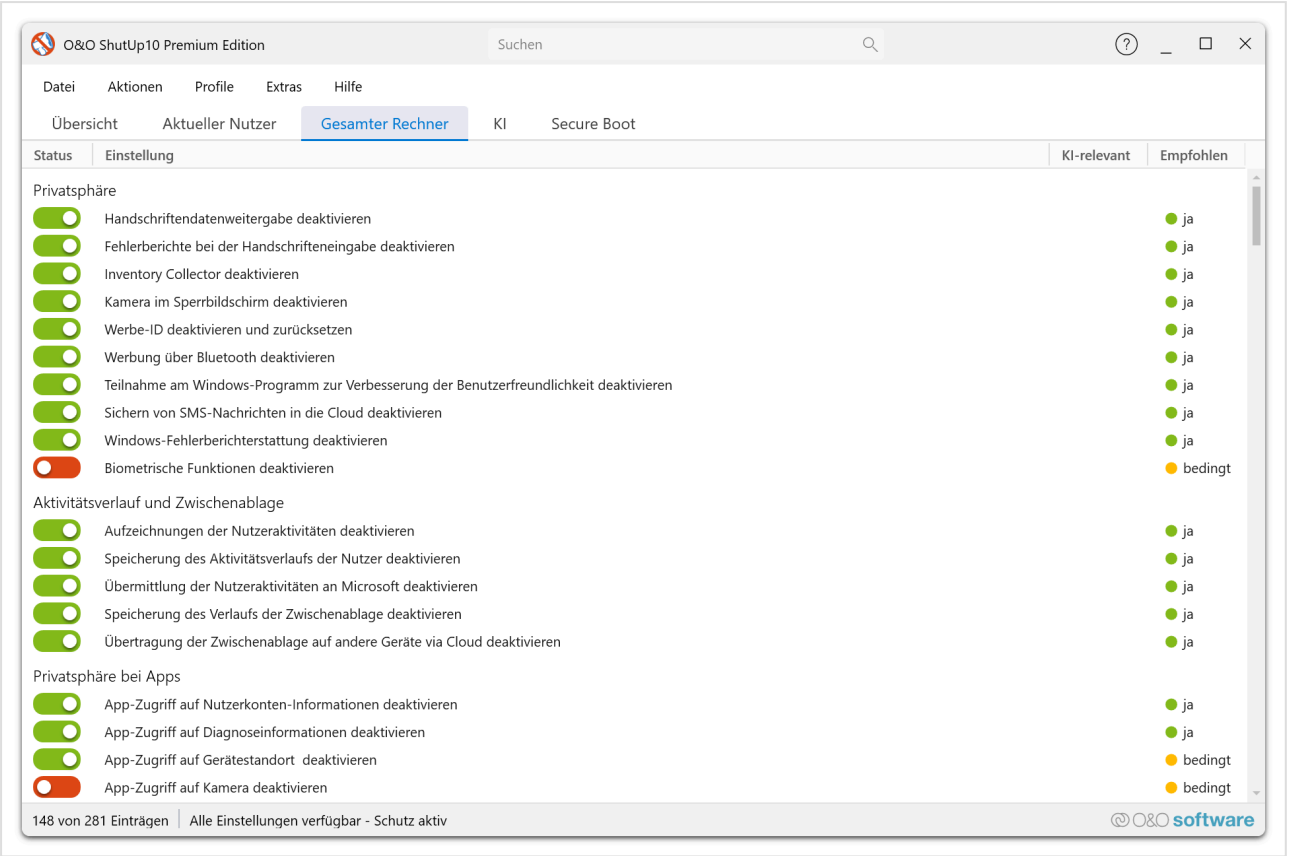


Diese Registerkarte ist nur in der Premium Edition verfügbar.

Option	Beschreibung
Nicht automatisch starten	Die Anwendung startet nicht automatisch, wenn Sie sich bei Windows anmelden.
Automatisch für aktuellen Benutzer starten	Die Anwendung startet automatisch, wenn der aktuelle Benutzer sich anmeldet.
Automatisch für alle Benutzer starten	Die Anwendung startet automatisch für alle Benutzer auf dem Computer. Erfordert erhöhte Berechtigungen.

Die folgenden Beispiele veranschaulichen die Autostart-Optionen, wie sie in der Client-Oberfläche erscheinen:

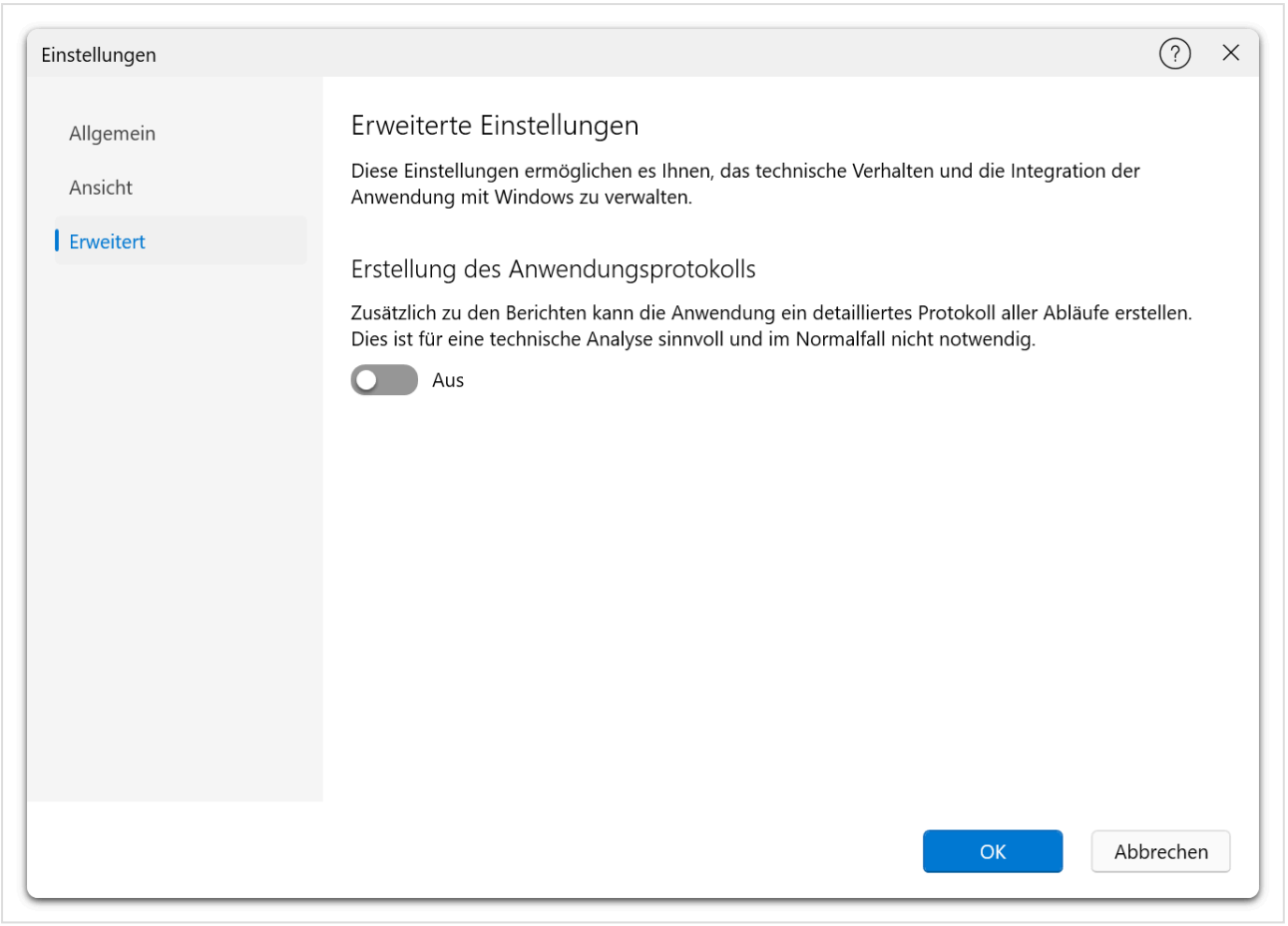

O&O ShutUp10 Premium Edition
Suchen
Datei
Aktionen
Profile
Extras
Hilfe
Übersicht
Aktueller Nutzer
Gesamter Rechner
KI
Secure Boot
Status
Einstellung
KI-relevant
Empfohlen
Privatsphäre
Werbe-ID deaktivieren und zurücksetzen
ja
Übermittlung von Schreibinformationen deaktivieren
ja
Gelegentliche Vorschläge in der Zeitachse deaktivieren
ja
Gelegentliche Vorschläge im Startmenü deaktivieren
ja
Tipps, Tricks und Vorschläge bei der Nutzung von Windows deaktivieren
ja
Anzeige von vorgeschlagenen Inhalten in den Systemeinstellungen deaktivieren
ja
Möglichkeit des Vorschlagens zum Abschließen der Einrichtung des Gerätes deaktivieren
ja
App-Benachrichtigungen deaktivieren
bedingt
Zugriff auf Sprachliste des Browsers deaktivieren
bedingt
Textvorschläge bei der Bildschirmtastatur deaktivieren
bedingt
Senden der URLs aus Apps an Windows Store deaktivieren
nein
Aktivitätsverlauf und Zwischenablage
Speicherung des Verlaufs der Zwischenablage deaktivieren
ja
Privatsphäre bei Apps
App-Zugriff auf Nutzerkonten-Informationen deaktivieren
ja
Verfolgung der App-Starts durch Windows deaktivieren
ja
App-Zugriff auf Diagnoseinformationen deaktivieren
ja
App-Zugriff auf Gerätestandort deaktivieren
bedingt
App-Zugriff auf Kamera deaktivieren
bedingt
App-Zugriff auf Mikrofon deaktivieren
bedingt
App-Zugriff auf Sprachaktivierung deaktivieren
bedingt
133 von 281 Einträgen
Alle Einstellungen verfügbar - Schutz aktiv
O&O software



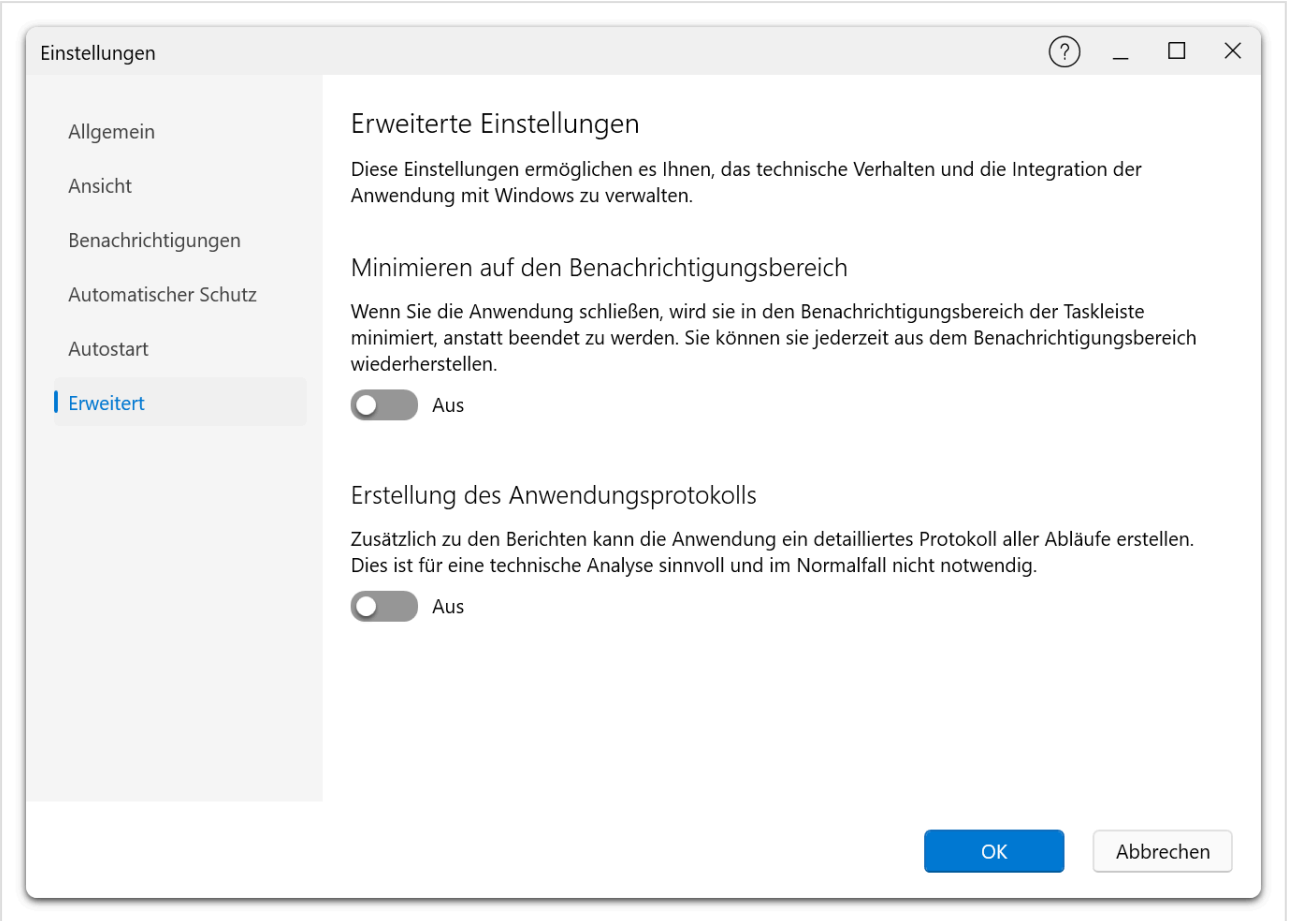
Registerkarte „Erweitert"

Diese Einstellungen ermöglichen es Ihnen, das technische Verhalten und die Integration der Anwendung mit Windows zu verwalten.

Free Edition:



Premium Edition:



In Benachrichtigungsbereich minimieren Premium

Wenn aktiviert, wird die Anwendung beim Schließen in den Benachrichtigungsbereich (Systemleiste) minimiert, anstatt zu beenden. Sie können sie jederzeit über das Symbol im Benachrichtigungsbereich wiederherstellen. Dies ist eine Nur-Premium-Funktion.

Protokollierung aktivieren

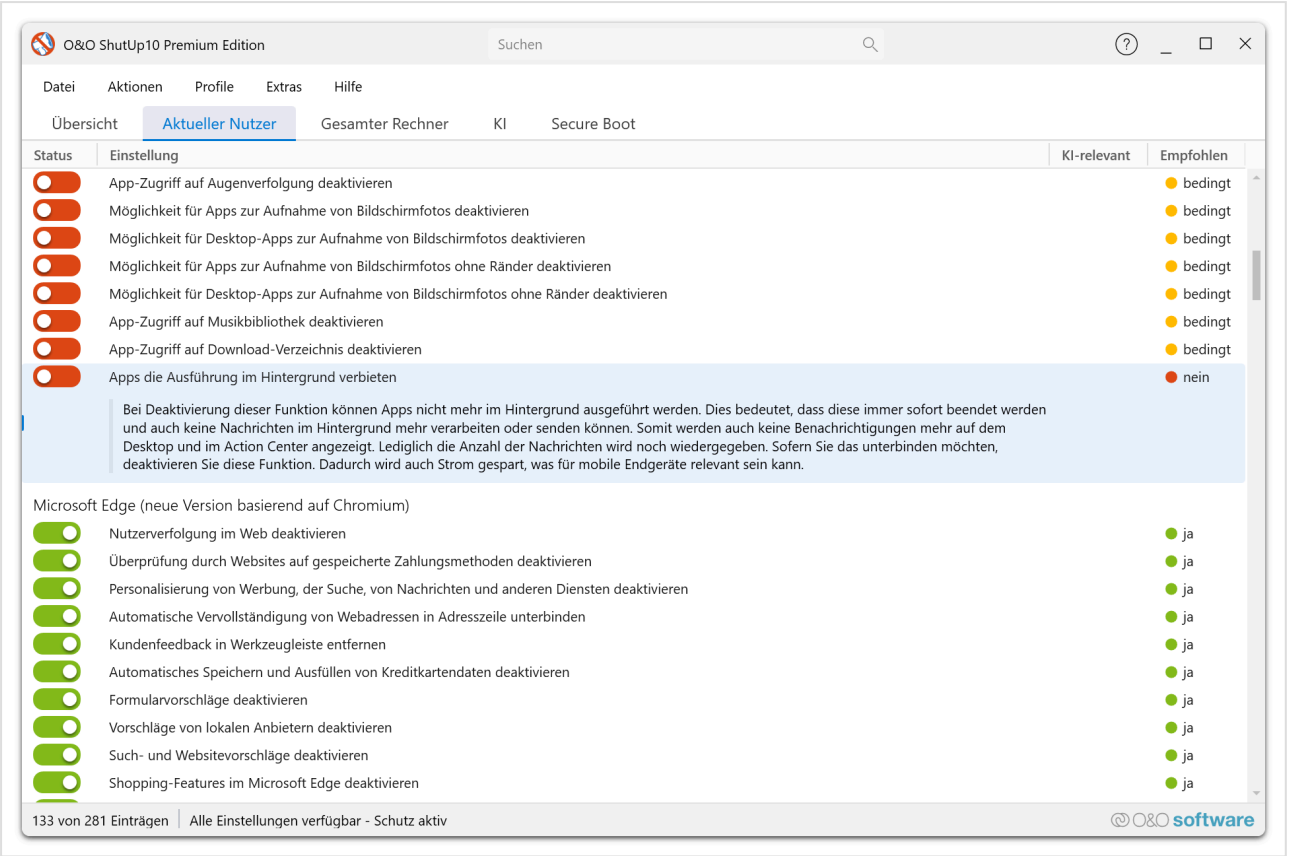
Zusätzlich zu den Standardberichten kann die Anwendung ein detailliertes Protokoll aller Operationen erstellen. Dies ist nützlich für technische Analyse und Fehlerbehebung. Die Protokollierung ist in BlueCon- und Fortress-Modus-Builds ausgeblendet.

Update-Überprüfung

Konfigurieren Sie, ob die Anwendung beim Start automatisch nach neuen Versionen sucht. Wenn aktiviert, kontaktiert die Anwendung den O&O Software-Update-Server, um festzustellen, ob eine neuere Version verfügbar ist. Wenn eine neuere Version gefunden wird, wird eine Benachrichtigung mit einer Option zum Herunterladen des Updates angezeigt. Deaktivieren Sie diese Option, wenn Sie Updates lieber manuell überprüfen oder Ihre Umgebung ausgehende Netzwerkverbindungen einschränkt.

Registerkarte „Information"

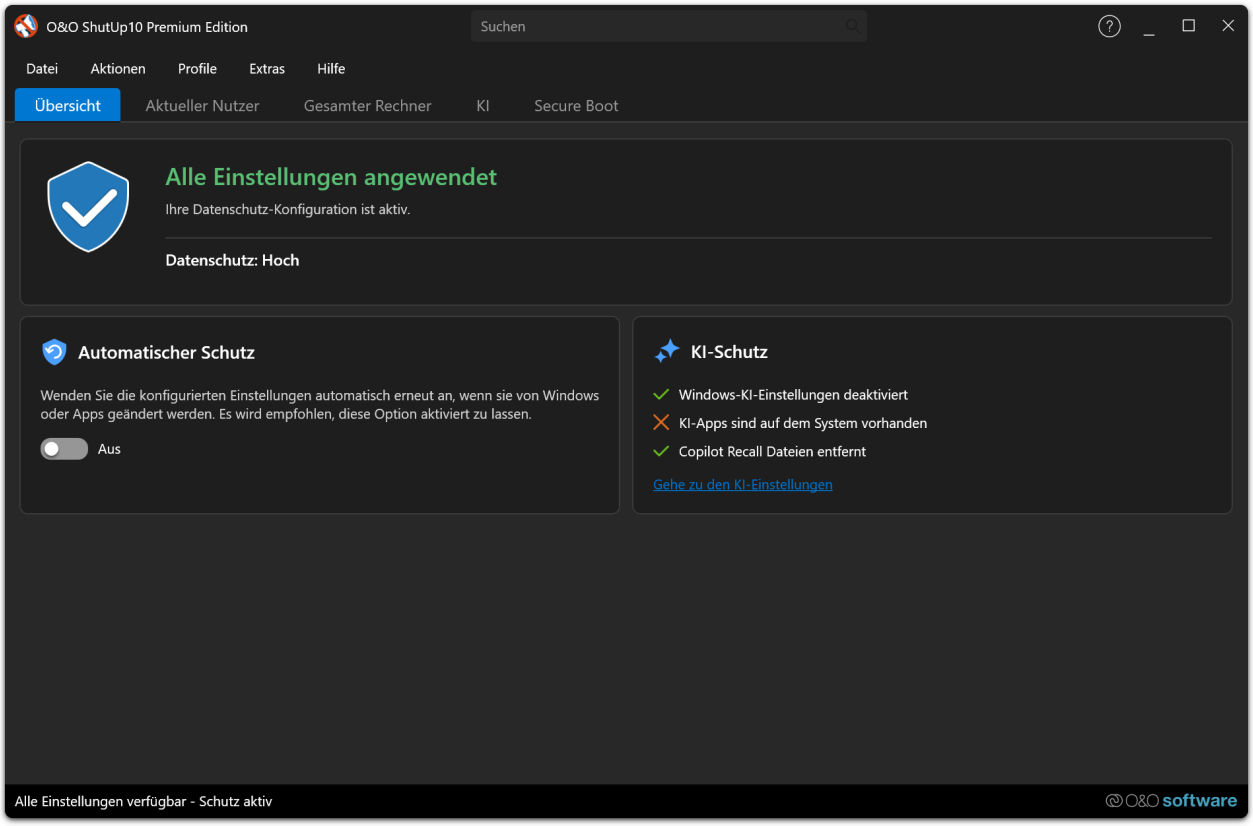
Zeigt Versionsinformationen und Produktdetails über die Anwendung an.



Die Registerkarte „Information" bietet eine schnelle Referenz für die installierte Version von O&O ShutUp10, einschließlich Editionstyp, Build-Nummer und Urheberrechtsinformationen. Dies ist nützlich zur Überprüfung Ihrer Installation bei der Kontaktaufnahme mit dem Support oder zur Überprüfung der Kompatibilität.

Automatischer Schutz Premium

Automatischer Schutz ist eine exklusive Funktion der **O&O ShutUp10 Premium Edition**. Er stellt sicher, dass Ihre Datenschutzeinstellungen auch nach Windows-Updates, Gruppenrichtlinienänderungen oder anderen Systemänderungen angewendet bleiben.



Überblick

Windows-Updates setzen häufig Datenschutzeinstellungen auf ihre Standards zurück. In der Free Edition müssen Benutzer ihre bevorzugten Einstellungen nach jedem Update manuell überprüfen und erneut anwenden. Die Premium Edition löst dies mit dem Automatischen Schutz.

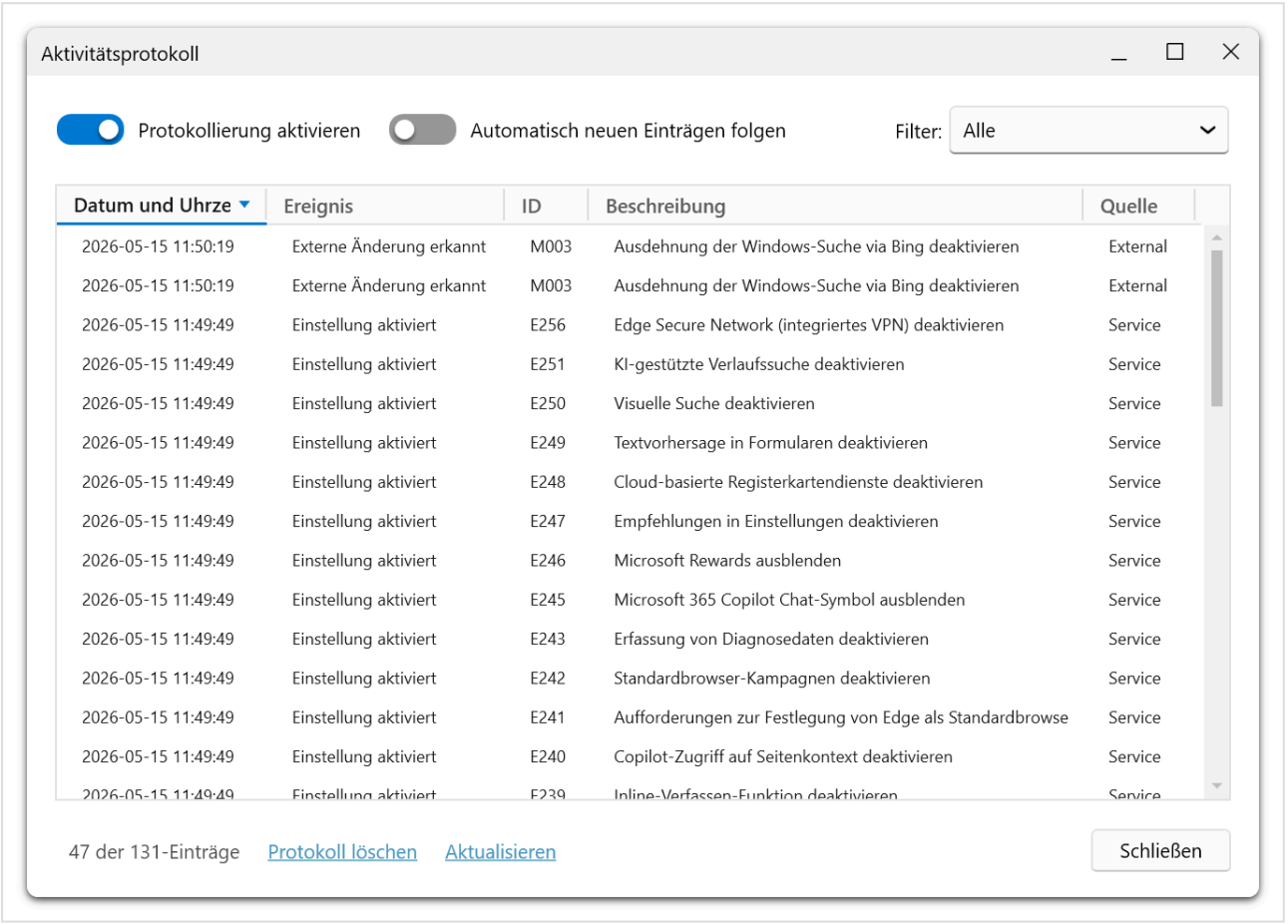
Funktionsweise

Der O&O ShutUp10-Dienst läuft im Hintergrund und überwacht kontinuierlich Ihre Datenschutzeinstellungen. Wenn er eine Änderung erkennt — sei es durch ein Windows-Update, eine Gruppenrichtlinien-Aktualisierung oder eine andere Systemänderung — wendet er Ihre bevorzugte Konfiguration automatisch erneut an.

Überwachte Ereignisse

Der Dienst reagiert auf:

- **Windows-Updates** — Einstellungen, die während eines kumulativen oder Feature-Updates zurückgesetzt wurden, werden wiederhergestellt.
- **Gruppenrichtlinienänderungen** — Wenn eine Richtlinienüberschreibung mit Ihren Einstellungen in Konflikt steht, wendet der Dienst Ihre Einstellungen erneut an.
- **Registry-Änderungen** — Direkte Änderungen an datenschutzrelevanten Registry-Werten werden erkannt und korrigiert.



Konfiguration

Sie konfigurieren Ihre bevorzugten Datenschutzeinstellungen einmal über die Client-Anwendung. Der Dienst speichert diese Konfiguration und verwendet sie als Basis für den Automatischen Schutz.

> **Info**
>
> Der Automatische Schutz erfordert, dass der O&O ShutUp10-Dienst ausgeführt wird. Wenn der Dienst gestoppt ist, werden Einstellungen nicht automatisch erneut angewendet, bis der Dienst neu gestartet wird.

Vorteile

- **Einmal einstellen und vergessen** — Einmal konfigurieren, kontinuierlich geschützt bleiben.
- **Schutz vor Update-Rückschritten** — Windows-Updates machen Ihre Datenschutzentscheidungen nicht mehr stillschweigend rückgängig.
- **Kein Benutzereingriff erforderlich** — Der Dienst erledigt alles im Hintergrund.

Profil-Editor Premium

Der Profil-Editor ist eine exklusive Funktion der **O&O ShutUp10 Premium Edition**. Er bietet eine vollständige Verwaltungsoberfläche zum Erstellen, Organisieren und Anwenden von Datenschutzeinstellungsprofilen.

Überblick

Profile ermöglichen es Ihnen, einen bestimmten Satz von Datenschutzeinstellungen zu speichern und jederzeit erneut anzuwenden. Der Profil-Editor (erreichbar über **Profile → Benutzerdefinierte Profile…** im Hauptmenü) ermöglicht die Verwaltung sowohl eingebauter Standardprofile als auch Ihrer eigenen benutzerdefinierten Profile.

Eingebaute Standardprofile

Der Profil-Editor enthält mehrere eingebaute Standardprofile, die fertige Datenschutzkonfigurationen für gängige Szenarien bieten. Diese Profile sind schreibgeschützt und können nicht geändert oder gelöscht werden.

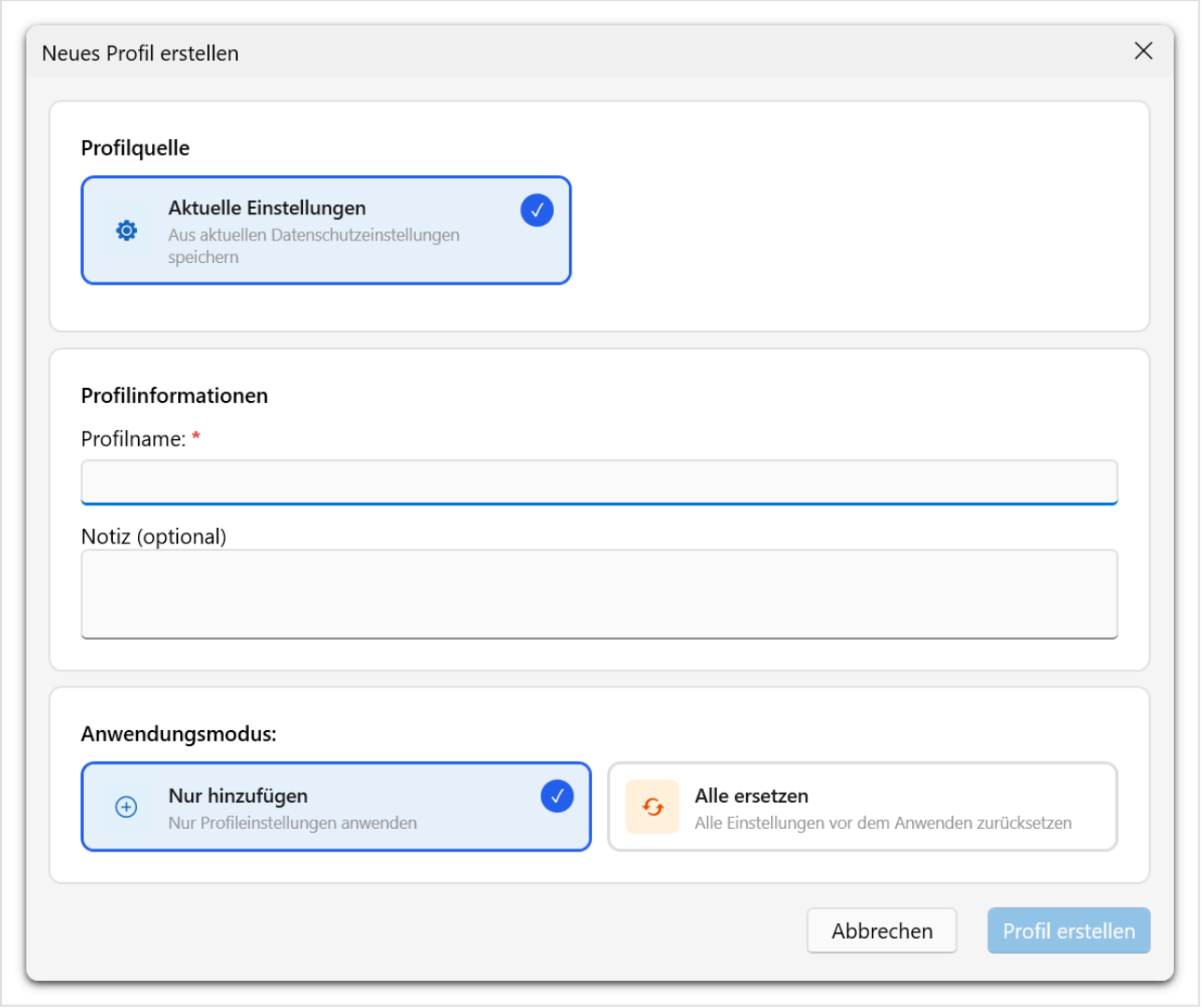
Profil	Beschreibung
Empfohlene Einstellungen	Aktiviert alle empfohlenen Datenschutzeinstellungen. Sicher für die meisten Benutzer mit minimaler Auswirkung auf die Funktionalität.
Eingeschränkte Einstellungen	Aktiviert alle eingeschränkt empfohlenen Datenschutzeinstellungen. Erweiterter Datenschutz, der einige Windows-Funktionen beeinträchtigen kann.
Kritische Einstellungen	Aktiviert alle kritischen Datenschutzeinstellungen. Maximaler Datenschutz, der die Funktionalität erheblich beeinträchtigen kann.
Empfohlene + Eingeschränkte Einstellungen	Aktiviert alle empfohlenen und eingeschränkt empfohlenen Datenschutzeinstellungen. Erweiterter Datenschutz, der einige Windows-Funktionen beeinträchtigen kann.
Alle Einstellungen (Maximaler Datenschutz)	Aktiviert alle Datenschutzeinstellungen über empfohlene, eingeschränkte und kritische Kategorien hinweg. Maximaler Datenschutz, der die Funktionalität erheblich beeinträchtigen kann.
Werkseinstellungen	Setzt alle Datenschutzeinstellungen auf Windows-Werksstandards zurück. Stellt das ursprüngliche Systemverhalten wieder her.
Vom BSI empfohlene Einstellungen	Wendet alle vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Einstellungen zur Deaktivierung von Funktechnologien, Telemetrie und verwandten Funktionen in Windows 10/11 an.

> **Caution**
>
> Eingebaute Profile, die als **schreibgeschützt** gekennzeichnet sind, können nicht umbenannt, bearbeitet oder gelöscht werden. Sie werden von der Anwendung gepflegt und mit neuen Versionen aktualisiert.

Benutzerdefinierte Profile erstellen

Benutzerdefinierte Profile werden im **Bearbeitungsmodus** erstellt (siehe Bearbeitungsmodus). Der Arbeitsablauf ist:

1. **Bearbeitungsmodus aktivieren** über das Bearbeiten-Menü.
2. **Einstellungen umschalten**, um den gewünschten Datenschutzstatus zu konfigurieren — Änderungen werden gepuffert und nicht sofort angewendet.
3. **Als Profil speichern** über das Bearbeiten-Menü — der Dialog „Benutzerdefiniertes Profil speichern" öffnet sich.
4. Einen **Profilnamen** (erforderlich) und eine optionale **Beschreibung/Notiz** eingeben.
5. Auf **Profil erstellen** klicken, um zu speichern.



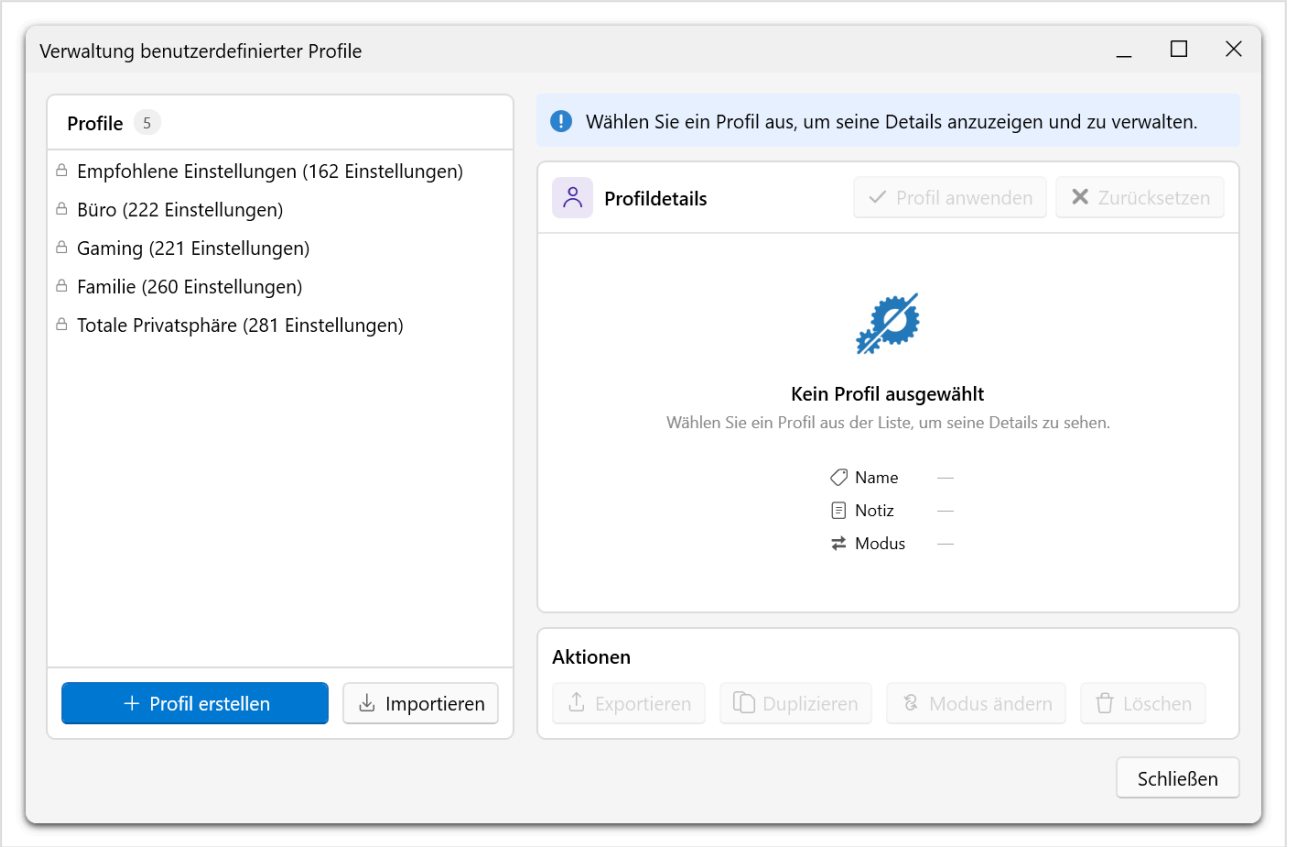
Das Profil speichert alle gepufferten Einstellungsänderungen. Sie können mehrere Profile für verschiedene Szenarien erstellen (z.B. ein strenges Profil für den persönlichen Gebrauch und ein ausgewogenes Profil für einen gemeinsam genutzten Arbeitsplatz).

Validierungsregeln

- Ein Profilname ist erforderlich. Ein leerer Name wird nicht akzeptiert.
- Doppelte Profilnamen sind nicht erlaubt.
- Sie müssen mindestens eine gepufferte Änderung haben, bevor Sie speichern können.

Profile verwalten

Der Dialog **Benutzerdefinierte Profile verwalten** (erreichbar über **Profile → Benutzerdefinierte Profile…**) bietet eine Zwei-Panel-Oberfläche:



Linkes Panel — Profilliste

Zeigt alle verfügbaren Profile (eingebaute und benutzerdefinierte) mit einer Profilanzahl-Kopfzeile an. Wählen Sie ein Profil aus, um seine Details anzuzeigen.

Rechtes Panel — Profildetails und Aktionen

Zeigt die Metadaten des ausgewählten Profils:

- **Profilname**
- **Erstellungsdatum**
- **Anzahl der Einstellungen** im Profil
- **Notiz/Beschreibung**

Verfügbare Aktionen für benutzerdefinierte Profile:

Aktion	Beschreibung
Profil anwenden	Wendet alle Einstellungen des ausgewählten Profils auf das System an.
Umbenennen	Ändert den Profilnamen.
Notiz bearbeiten	Ändert die Profilbeschreibung.
Löschen	Entfernt das benutzerdefinierte Profil dauerhaft.

> **Info**
>
> Eingebaute Standardprofile unterstützen nur die Aktion **Profil anwenden**. Umbenennen, Notiz bearbeiten und Löschen sind für eingebaute Profile nicht verfügbar.

Profil anwenden

Wenn Sie ein Profil anwenden, werden alle im Profil enthaltenen Datenschutzeinstellungen auf das System angewendet. Bei eingebauten Profilen werden Einstellungen gemäß ihrer Empfehlungsstufe angewendet. Bei benutzerdefinierten Profilen werden die beim Erstellen des Profils erfassten exakten Einstellungszustände wiederhergestellt.

> **Tip**
>
> Bevor Sie ein Profil anwenden, das viele Einstellungen ändert, erstellen Sie einen Systemwiederherstellungspunkt über das **Aktionen**-Menü. Dies ermöglicht es Ihnen, alle Änderungen bei Bedarf einfach rückgängig zu machen.

Premium-Übersicht Premium

Die **Premium-Übersicht** ist eine Seite mit doppelter Funktion in der O&O ShutUp10 Premium Edition, die sowohl als Einstiegspunkt für die Ersteinrichtung als auch als laufendes Status-Dashboard dient. Sie wird im Hauptfenster als primäre Registerkarte angezeigt, wenn die Premium Edition ausgeführt wird.

Überblick

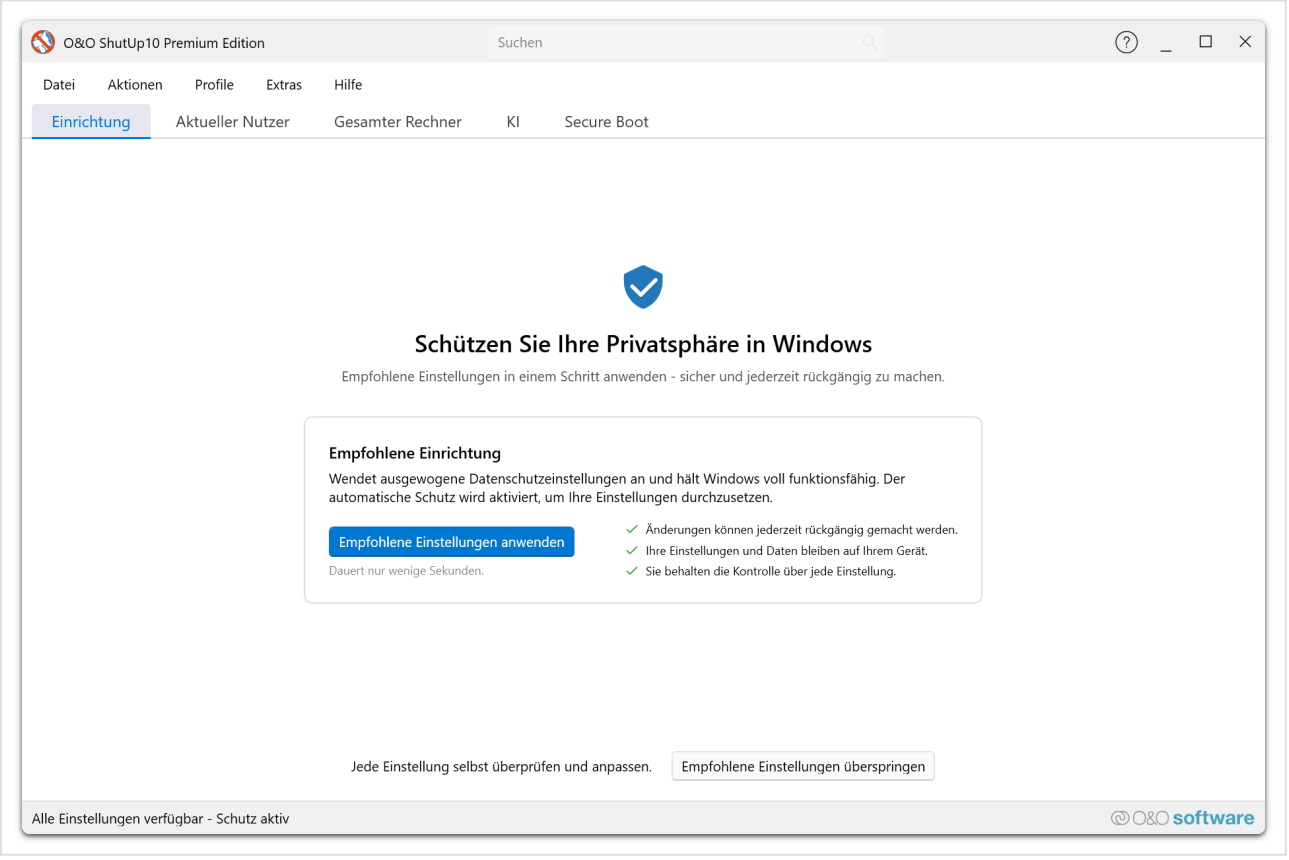
Die Premium-Übersicht arbeitet in zwei verschiedenen Modi, abhängig vom aktuellen Status der Anwendung:

- **Setup-Modus** — Wird angezeigt, wenn die Premium Edition noch nicht vollständig konfiguriert wurde (z.B. nach einer Neuinstallation oder wenn der Hintergrunddienst noch nicht verbunden ist).
- **Übersichtsmodus** — Wird angezeigt, sobald die Ersteinrichtung abgeschlossen ist und der Dienst läuft, und bietet eine Echtzeit-Zusammenfassung des Schutzstatus und wichtiger Kennzahlen.

Die Seite wechselt automatisch vom Setup-Modus in den Übersichtsmodus, sobald alle erforderlichen Konfigurationsschritte abgeschlossen sind.

Setup-Modus

Der Setup-Modus führt den Benutzer durch die Erstkonfiguration der Premium Edition nach der Installation.



Wenn die Premium Edition zum ersten Mal gestartet wird — oder wenn der Hintergrunddienst noch nicht konfiguriert wurde — zeigt die Premium-Übersicht einen geführten Setup-Arbeitsablauf an. Dieser Modus stellt sicher, dass alle Voraussetzungen erfüllt sind, bevor der automatische Schutz beginnt.

Was der Setup-Modus abdeckt

Schritt	Beschreibung
Dienstinstallation	Überprüft, dass der O&O ShutUp10-Hintergrunddienst installiert und bei Windows registriert ist.
Dienstverbindung	Bestätigt, dass die Client-Anwendung mit dem Hintergrunddienst kommunizieren kann.
Erste Profilauswahl	Fordert den Benutzer auf, ein Datenschutzprofil (z.B. Empfohlene Einstellungen) als Basiskonfiguration auszuwählen.
Erste Anwendung	Wendet das ausgewählte Profil an, um die anfängliche Datenschutzkonfiguration auf dem System festzulegen.

Barrierefreiheit

Der Setup-Modus ist für Benutzer konzipiert, die möglicherweise keine Administratorrechte haben. Der Hintergrunddienst übernimmt alle privilegierten Operationen, sodass der Setup-Arbeitsablauf keine UAC-Erhöhung vom Endbenutzer erfordert.

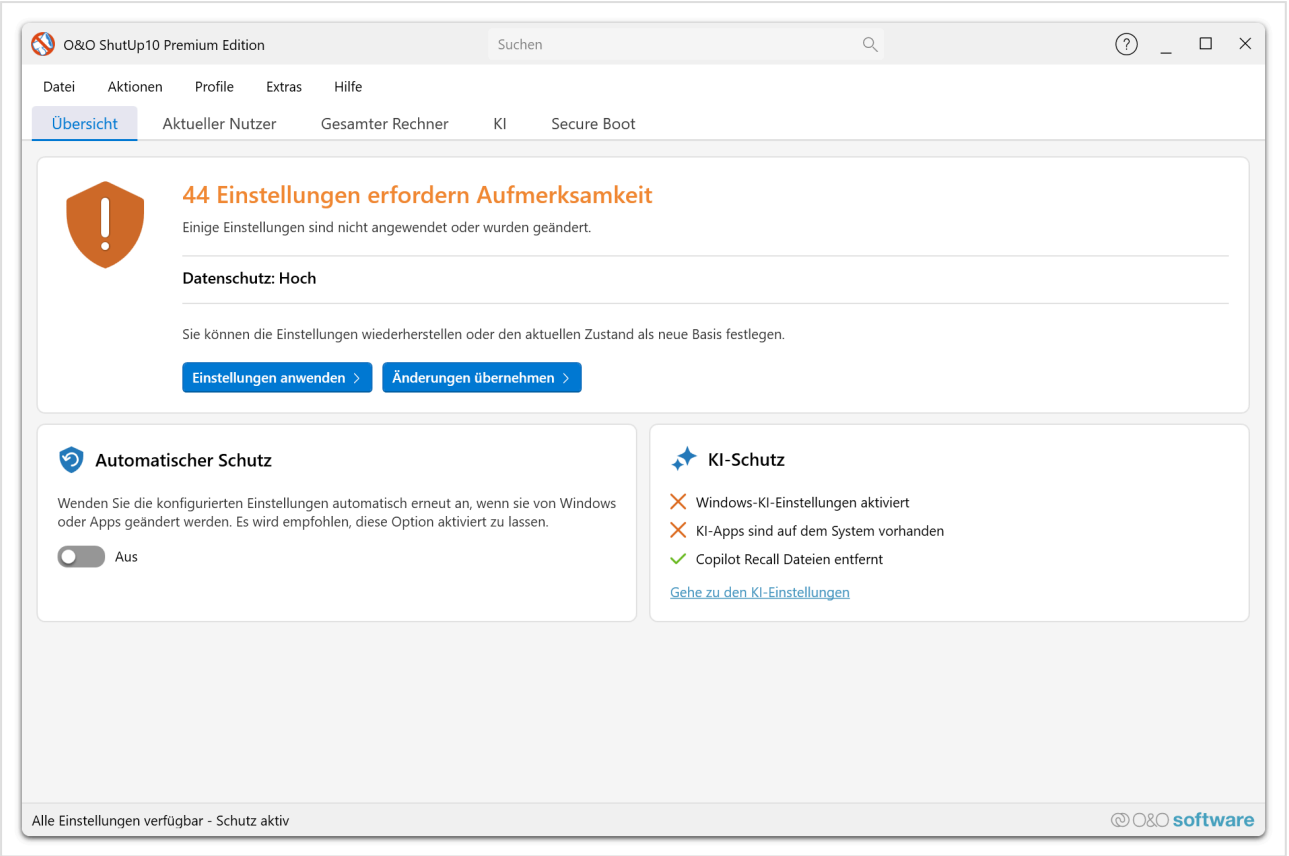
Wann der Setup-Modus erscheint

- Nach einer Neuinstallation der Premium Edition.
- Wenn der Hintergrunddienst deinstalliert oder nicht verfügbar ist.
- Wenn die Dienstverbindung verloren geht und nicht wiederhergestellt werden kann.

Sobald alle Setup-Schritte erfolgreich abgeschlossen sind, wechselt die Premium-Übersicht automatisch in den Übersichtsmodus.

Übersichtsmodus

Der Übersichtsmodus bietet ein Echtzeit-Dashboard des aktuellen Schutzstatus und der Dienstgesundheit.



Sobald die Premium Edition vollständig konfiguriert ist, zeigt die Premium-Übersicht eine Zusammenfassungsansicht, die Benutzern sofortige Sichtbarkeit in den Status ihres Datenschutzes gibt.

Dashboard-Elemente

Element	Beschreibung
Schutzstatus	Zeigt an, ob der automatische Schutz derzeit aktiv ist und die konfigurierte Datenschutzeinstellungen durchsetzt.
Dienststatus	Zeigt, ob der Hintergrunddienst läuft, gestoppt oder nicht verfügbar ist.
Aktives Profil	Zeigt den Namen des aktuell angewendeten Datenschutzprofils an.
Letzte Durchsetzung	Zeitstempel der letzten automatischen Neuanwendung von Datenschutzeinstellungen durch den Dienst.
Ausstehende Änderungen	Anzahl der Einstellungen, die vom konfigurierten Profil abweichen und für die Neuanwendung vorgemerkt sind.

Anwendungsszenarien

- **Tägliche Statusprüfung** — Öffnen Sie die Anwendung und sehen Sie sofort, ob der Schutz aktiv und der Dienst gesund ist.
- **Überprüfung nach Updates** — Überprüfen Sie nach einem Windows-Update, ob der Dienst Ihre Datenschutzeinstellungen automatisch erneut angewendet hat.

- **Fehlerbehebung** — Wenn der Dienststatus als gestoppt oder nicht verfügbar angezeigt wird, bietet die Übersicht einen Ausgangspunkt für die Diagnose von Verbindungs- oder Dienstproblemen.

Barrierefreiheit

Der Übersichtsmodus verwendet kontrastreiche Statusindikatoren und klare Beschriftungen, um die Lesbarkeit über alle unterstützten App-Ansichtsmodi hinweg sicherzustellen, einschließlich der Designs „Hoher Kontrast Schwarz" und „Hoher Kontrast Weiß". Statusinformationen werden in einem strukturierten Layout präsentiert, das mit Bildschirmleseprogrammen kompatibel ist.

Beziehung zu anderen Funktionen

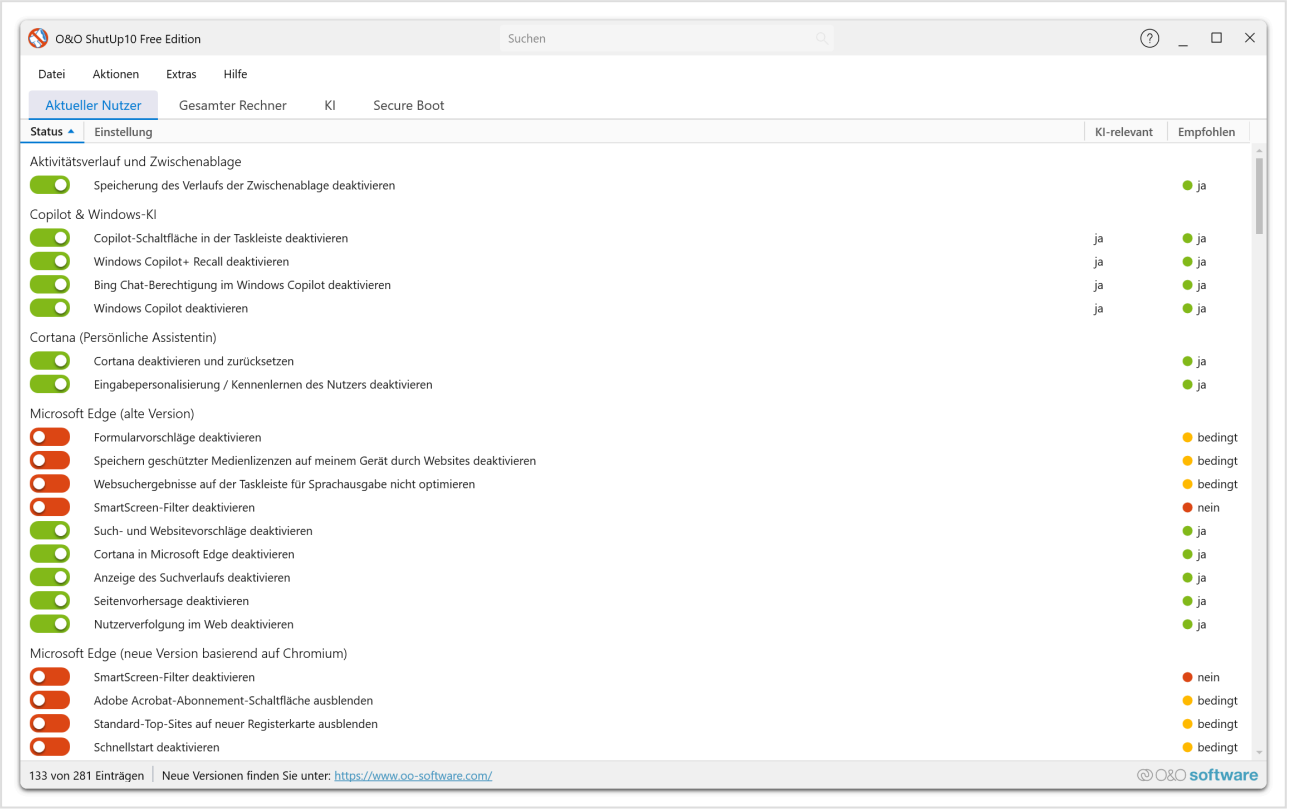
Die Premium-Übersicht integriert sich mit mehreren anderen Premium Edition-Funktionen:

- **Automatischer Schutz** — Der Schutzstatus und die letzte Durchsetzungszeit spiegeln den Status des Automatischen Schutzdienstes wider.
- **Profil-Editor** — Das im Übersichtsmodus angezeigte aktive Profil entspricht dem über den Profil-Editor verwalteten Profil.
- **Einstellungsdialog** — Dienstbezogene Konfiguration (Benachrichtigungen, Hybrid-Modus, Autostart) wird über den Einstellungsdialog verwaltet.

> **Tip**
>
> Wenn die Premium-Übersicht nach der Installation im Setup-Modus verbleibt, überprüfen Sie, ob der O&O ShutUp10-Dienst installiert ist und ausgeführt wird. Prüfen Sie die **Windows-Dienste** (services.msc) oder wenden Sie sich an Ihren IT-Administrator.

Datenschutzeinstellungen

O&O ShutUp10 bietet umfassende Kontrolle über fast 300 Windows-Datenschutzeinstellungen in mehr als 20 Kategorien. Dieser Abschnitt behandelt alle Einstellungskategorien, die in der Free und Premium Edition verfügbar sind.



Überblick

Windows 10 und Windows 11 enthalten zahlreiche datenschutzrelevante Einstellungen, die über die Einstellungs-App, Gruppenrichtlinien und die Windows-Registry verteilt sind. O&O ShutUp10 fasst diese in einer einzigen Oberfläche zusammen und erleichtert die Überprüfung und Anpassung. Einstellungen sind in klar definierte Kategorien unterteilt, jede mit individuellen Empfehlungsstufen.

Empfehlungsstufen

Jede Datenschutzeinstellung enthält eine Empfehlungsstufe:

Stufe	Beschreibung
Empfohlen	Sicher für die meisten Benutzer. Keine negativen Auswirkungen auf die Kernfunktionalität.
Eingeschränkt	Grundsätzlich sicher, kann aber bestimmte Personalisierungsfunktionen beeinträchtigen.
Nicht empfohlen	Kann wichtige Funktionalität beeinträchtigen. Nur mit Verständnis der Auswirkungen anwenden.

> **Tip**
>
> Beginnen Sie mit dem Anwenden der **Empfohlenen** Einstellungen. Sie können einzelne Einstellungen jederzeit später anpassen.

Einstellungskategorien

Datenschutz

Steuert grundlegende Windows-Datenschutzverhalten einschließlich Fehlerberichterstattung, Benachrichtigungen und Vorschläge. Diese Einstellungen verhindern, dass Windows persönliche Informationen überträgt und unerwünschte Inhalte anzeigt.

Wichtige empfohlene Einstellungen:

- **Windows-Fehlerberichterstattung deaktivieren** — Verhindert das Hochladen von Absturzberichten (die Speicherauszüge mit persönlichen Daten enthalten können) an Microsoft.
- **Tipps, Tricks und Vorschläge bei der Verwendung von Windows deaktivieren** — Unterdrückt Popup-Meldungen im Benachrichtigungsbereich und Info-Center.
- **Vorgeschlagene Inhalte in der Einstellungs-App deaktivieren** — Verhindert Werbevorschläge in den Systemeinstellungen.
- **Vorschläge in der Zeitleiste deaktivieren** — Blockiert Werbung in der Windows Explorer-Zeitleiste (z.B. OneDrive-Werbung).
- **App-Benachrichtigungen deaktivieren** — Verhindert, dass Apps Benachrichtigungen auf Kacheln, Sperrbildschirm und Desktop anzeigen.

Telemetrie und Benutzerverhalten

Verwaltet die Diagnose- und Telemetriedaten, die Windows zur Produktverbesserung an Microsoft sendet. Das Deaktivieren dieser Einstellungen reduziert die Menge an Nutzungsdaten, Absturzberichten und Verhaltensanalysen, die von Ihrem Gerät übertragen werden, erheblich.

Wichtige empfohlene Einstellungen:

- **Anwendungstelemetrie deaktivieren** — Stoppt das Senden von Nutzungsdaten und Absturzinformationen an Microsoft.
- **Anpassung der Benutzererfahrung durch Diagnosedaten deaktivieren** — Verhindert, dass Microsoft Ihre Diagnosedaten zur Personalisierung nutzt.
- **Sammlung von Diagnoseprotokollen deaktivieren** — Stoppt die Erfassung detaillierter Diagnoseprotokolle.
- **Download von OneSettings-Konfigurationseinstellungen deaktivieren** — Verhindert, dass Microsoft Ihr Gerät fernkonfiguriert.

App-Datenschutz

Steuert, auf welche Systemressourcen und persönliche Daten Windows-Apps zugreifen können. Dies umfasst Sprachaktivierung, Kamera, Mikrofon, Kontakte, Kalender, Nachrichten und mehr. Die Einschränkung von App-Berechtigungen begrenzt, welche

Informationen Apps von Drittanbietern und integrierten Apps sammeln können.

Wichtige empfohlene Einstellungen:

- **App-Zugriff auf Sprachaktivierung deaktivieren** — Verhindert, dass Apps durch Sprachbefehle aktiviert werden.
- **App-Zugriff auf Benutzerkontoinformationen deaktivieren** — Blockiert Apps beim Lesen Ihres Kontonamens und Profilbilds.
- **App-Zugriff auf Videos deaktivieren** — Verhindert, dass Apps auf Ihre Videobibliothek zugreifen.
- **App-Zugriff auf Sprachaktivierung bei gesperrtem Gerät deaktivieren** — Blockiert sprachaktivierten App-Zugriff bei gesperrtem Gerät.

Cortana (Persönlicher Assistent)

Steuert Cortana und Eingabepersonalisierungsfunktionen. Diese Einstellungen verhindern, dass Microsoft Sprach-, Handschrift- und Tastatureingabedaten sammelt, die zum Training von Cortana und zur Verbesserung der Erkennung verwendet werden.

Wichtige empfohlene Einstellungen:

- **Eingabepersonalisierung deaktivieren** — Stoppt die Sammlung von Sprach-, Handschrift- und Tastatureingabedaten durch Microsoft.
- **Suchhervorhebungen in der Taskleiste deaktivieren** — Entfernt visuelle Suchhervorhebungen, die mit Microsoft-Servern kommunizieren.
- **Websuche in Cortana deaktivieren** — Verhindert, dass Suchanfragen an Bing gesendet werden.

Standortdienste

Steuert, wie Windows und Apps Ihren physischen Standort nutzen. Das Deaktivieren von Standortdiensten verhindert GPS-, Wi-Fi- und sensorbasierte Standortverfolgung, was wiederum verhindert, dass Standortdaten an Microsoft und Apps von Drittanbietern gesendet werden.

Wichtige empfohlene Einstellungen:

- **App-Zugriff auf Ihren Standort deaktivieren** — Verhindert, dass Apps auf Ihren physischen Standort zugreifen.
- **Sensoren zur Standortbestimmung und Orientierung deaktivieren** — Deaktiviert GPS- und Gyroskop-Sensoren (kann die Bildschirmrotation auf Tablets beeinträchtigen).
- **Funktionalität zur Standortbestimmung des Systems deaktivieren** — Blockiert die Standortverfolgung auf Systemebene.
- **Skript-Funktionalität zur Standortbestimmung deaktivieren** — Verhindert skriptbasierte Standorterkennung.

Suche

Steuert das Verhalten der Windows-Suche, einschließlich Websuche-Integration und Sammlung des Suchverlaufs.

Wichtige empfohlene Einstellungen:

- **Websuche im Startmenü deaktivieren** — Verhindert, dass Startmenü-Suchanfragen an Bing gesendet werden.

Synchronisierung von Windows-Einstellungen

Verwaltet die Synchronisierung Ihrer Windows-Einstellungen über Geräte hinweg unter Verwendung eines Microsoft-Kontos. Einstellungen, Passwörter, Spracheinstellungen und Designentscheidungen werden auf Microsoft-Servern gespeichert, wenn die Synchronisierung aktiv ist.

Wichtige empfohlene Einstellungen:

- **Synchronisierung aller Einstellungen deaktivieren** — Stoppt die Synchronisierung aller Windows-Einstellungen mit Microsoft-Servern.

- **Synchronisierung von Anmeldeinformationen (Passwörtern) deaktivieren** — Verhindert, dass Passwörter über Microsoft-Server gespeichert und synchronisiert werden.
- **Synchronisierung von Spracheinstellungen deaktivieren** — Stoppt die gemeinsame Nutzung von Spracheinstellungen über Geräte hinweg.
- **Synchronisierung von Designeinstellungen deaktivieren** — Verhindert die Synchronisierung von Design- und visuellen Einstellungen.

Sicherheit

Steuert sicherheitsbezogene Funktionen, die sich mit dem Datenschutz überschneiden, einschließlich Wi-Fi Sense, DRM, dem Schrittaufzeichner und dem Programm zur Verbesserung der Kundenzufriedenheit. Die Anpassung dieser Einstellungen reduziert die an Microsoft geteilten Daten bei gleichzeitiger Aufrechterhaltung der Kernsicherheit.

Wichtige empfohlene Einstellungen:

- **WiFi Sense deaktivieren** — Verhindert die automatische Verbindung zu Wi-Fi-Netzwerken von Kontakten und die Weitergabe Ihres Wi-Fi-Passworts über Microsoft-Server.
- **Benutzer-Schrittaufzeichner deaktivieren** — Stoppt die automatische Aufzeichnung aller Aktionen auf Ihrem Computer (einschließlich Screenshots und eingegebener Texte).
- **Internetzugriff von Windows Media Digital Rights Management (DRM) deaktivieren** — Blockiert DRM-bezogene Internetkommunikation (nur wenn Sie keine DRM-geschützten Medien verwenden).
- **Teilnahme am Programm zur Verbesserung der Kundenzufriedenheit deaktivieren** — Stoppt das Senden von Hardware- und Softwarenutzungsdaten an Microsoft.

Windows Update

Steuert, wie Windows Updates herunterlädt und installiert, einschließlich Peer-to-Peer-Bereitstellung, automatische Treiberupdates und optionale/Vorschau-Updates. Während Sicherheitsupdates kritisch sind, übertragen einige Update-Funktionen Daten oder installieren nicht wesentliche Inhalte.

Wichtige empfohlene Einstellungen:

- **Windows Update über Peer-to-Peer deaktivieren** — Verhindert, dass Ihr Computer Update-Daten mit anderen PCs über das Internet teilt.
- **Optionale Updates (einschließlich Vorschau-Updates) deaktivieren** — Verhindert die Installation unfertiger Vorschau-Updates.
- **Aufschieben von Upgrades aktivieren** — Verzögert Feature-Upgrades, damit Sie sie zu einem Zeitpunkt Ihrer Wahl installieren können.

Microsoft Edge (neue Version basierend auf Chromium)

Steuert Datenschutz- und Telemetrieeinstellungen speziell für den Chromium-basierten Microsoft Edge-Browser. Diese Einstellungen verwalten Datenerfassung, Autofill-Verhalten, Cloud-Dienste und Werbeinhalte innerhalb von Edge.

Wichtige empfohlene Einstellungen:

- **Automatische Anmeldung vom Web zum Browser deaktivieren** — Verhindert die automatische Browser-Anmeldung beim Anmelden auf Microsoft-Websites.
- **Visuelle Suche deaktivieren** — Stoppt das Senden von Bildern an Bing zur visuellen Suche.
- **Textvorhersage in Formularen deaktivieren** — Verhindert cloudbasierte Textvorhersage in Browser-Formularfeldern.
- **Cloudbasierte Tab-Dienste deaktivieren** — Stoppt die Synchronisierung von Tab-Daten mit Microsoft-Cloud-Diensten.
- **Microsoft Rewards ausblenden** — Entfernt Microsoft Rewards-Werbeinhalte aus dem Browser.

Microsoft Edge (ältere Version)

Steuert Datenschutzeinstellungen für die ältere (nicht-Chromium) Version von Microsoft Edge. Diese Einstellungen verwalten Formularvorschläge, Suchverlauf, Web-Tracking und die Edge-Leiste.

Wichtige empfohlene Einstellungen:

- **Tracking im Web deaktivieren** — Aktiviert Do-Not-Track-Signale im älteren Edge-Browser.
- **Formularvorschläge deaktivieren** — Verhindert, dass Edge Formulardaten speichert und vorschlägt.
- **Anzeige des Suchverlaufs deaktivieren** — Stoppt die Anzeige früherer Suchanfragen in Edge.
- **Edge-Leiste deaktivieren** — Entfernt die Edge-Leiste vom Desktop.

Microsoft Office

Steuert Datenschutz- und Telemetrieeinstellungen für Microsoft Office-Anwendungen. Diese Einstellungen verwalten verbundene Erfahrungen, Diagnosedaten und Feedback-Mechanismen, die Nutzungsinformationen an Microsoft übermitteln.

Wichtige empfohlene Einstellungen:

- **Verbundene Erfahrungen mit Inhaltsanalyse deaktivieren** — Stoppt das Senden eingegebener Daten an Microsofts Cloud zur Analyse durch Office.
- **Übermittlung von Diagnosedaten deaktivieren** — Verhindert, dass Office diagnostische Nutzungsdaten überträgt.
- **Microsoft Office-Umfragen deaktivieren** — Blockiert In-Product-Umfrage-Eingabeaufforderungen.
- **Teilnahme am Programm zur Verbesserung der Kundenzufriedenheit deaktivieren** — Stoppt das Senden von Office-Nutzungsdaten an Microsoft.

Microsoft 365

Zusätzliche Datenschutzeinstellungen speziell für Microsoft 365 Cloud-verbundene Funktionen und Dienste.

Windows Explorer

Steuert datenschutzrelevante Verhaltensweisen im Windows Explorer, einschließlich OneDrive-Integration, Startmenü-Vorschläge und Verfolgung zuletzt geöffneter Elemente.

Wichtige empfohlene Einstellungen:

- **Werbung in Windows Explorer/OneDrive deaktivieren** — Entfernt Werbung und Synchronisierungsanbieter-Benachrichtigungen aus dem Explorer.
- **Microsoft OneDrive deaktivieren** — Deaktiviert die Cloud-Speicher-Integration von Microsoft vollständig.
- **OneDrive-Zugriff auf das Netzwerk vor der Anmeldung deaktivieren** — Verhindert, dass OneDrive vor der Benutzeranmeldung synchronisiert.
- **Gelegentliche Anzeige von App-Vorschlägen im Startmenü deaktivieren** — Entfernt App-Werbung aus dem Startmenü.

Sperrbildschirm

Steuert die auf dem Windows-Sperrbildschirm angezeigten Informationen, einschließlich Benachrichtigungen, Werbung und Windows Spotlight-Inhalte, die mit Microsoft-Servern kommunizieren.

Wichtige empfohlene Einstellungen:

- **Wissenswertes, Tipps, Tricks und mehr auf dem Sperrbildschirm deaktivieren** — Entfernt Werbung und gesponserte Inhalte vom Sperrbildschirm.

- **Benachrichtigungen auf dem Sperrbildschirm deaktivieren** — Verhindert, dass potenziell private App-Benachrichtigungen ohne Anmeldung sichtbar sind.
- **Windows Spotlight deaktivieren** — Stoppt die Anzeige kuratierter Bilder und Inhalte von Microsoft auf dem Sperrbildschirm.

Taskleiste

Verwaltet Datenschutzeinstellungen für die Windows-Taskleiste, einschließlich Widgets, Suchfeld, Nachrichten-Feed und soziale Funktionen, die Daten mit Microsoft-Servern austauschen.

Wichtige empfohlene Einstellungen:

- **Widgets in Windows Explorer deaktivieren** — Verhindert den Datenaustausch von Windows 11-Widgets mit Microsoft-Servern.
- **Suchfeld in der Taskleiste deaktivieren** — Entfernt das Suchfeld, das Abfragen an Microsoft sendet.
- **Nachrichten und Interessen in der Taskleiste deaktivieren** — Entfernt den Nachrichten-Feed, der Browsing- und Interessendaten überträgt.
- **Personen-Symbol in der Taskleiste deaktivieren** — Entfernt die soziale Personen-Funktion aus der Taskleiste.

Aktivitätsverlauf und Zwischenablage

Steuert die Aufzeichnung von Benutzeraktivitäten und den Zwischenablageverlauf. Windows kann Ihre Aktivitäten über Apps und Geräte hinweg verfolgen und Zwischenablageninhalte für cloudbasiertes Teilen speichern.

Wichtige empfohlene Einstellungen:

- **Übermittlung von Benutzeraktivitäten an Microsoft deaktivieren** — Stoppt das Senden von Aktivitätsdaten an Microsoft-Server.
- **Speicherung des Aktivitätsverlaufs deaktivieren** — Verhindert, dass Windows Ihren Anwendungsnutzungsverlauf aufzeichnet.
- **Speicherung des Zwischenablageverlaufs deaktivieren** — Stoppt die Aufbewahrung von Zwischenablageninhalten durch Windows und reduziert potenzielle Sicherheitsrisiken.
- **Übertragung der Zwischenablage auf andere Geräte über die Cloud deaktivieren** — Verhindert die Synchronisierung von Zwischenablagedaten über Geräte hinweg über Microsoft-Server.

Microsoft Defender und Microsoft SpyNet

Steuert das Datenfreigabeverhalten von Microsoft Defender, einschließlich Probenübermittlung und SpyNet-Mitgliedschaft. Diese Einstellungen verwalten, welche sicherheitsbezogenen Daten zur Bedrohungsanalyse an Microsoft gesendet werden.

Wichtige empfohlene Einstellungen:

- **Übermittlung von Datenproben an Microsoft deaktivieren** — Verhindert, dass Defender Dateiproben zur Cloud-Analyse sendet.
- **Microsoft SpyNet-Mitgliedschaft deaktivieren** — Stoppt die Teilnahme am Microsoft SpyNet-Telemetrienetzwerk.
- **Meldung von Malware-Infektionsinformationen deaktivieren** — Verhindert das Senden von Malware-Erkennungsberichten an Microsoft.

> **Caution**
>
> Deaktivieren Sie Microsoft Defender selbst nicht, es sei denn, Sie haben eine alternative, regelmäßig aktualisierte Antivirenlösung installiert.

Microsoft Copilot (in Windows)

Steuert KI-bezogene Funktionen in Windows, einschließlich des Microsoft Copilot-Assistenten, der Copilot-Tastenkombination und KI-gestützter Funktionen in integrierten Apps wie Paint.

Wichtige empfohlene Einstellungen:

- **Windows Copilot deaktivieren** — Deaktiviert den Copilot KI-Assistenten in Windows vollständig.
- **Copilot-Schaltfläche aus der Taskleiste entfernen** — Entfernt die Copilot-Schaltfläche aus der Taskleiste.
- **Windows Copilot-Taste auf der Tastatur deaktivieren** — Verhindert, dass die dedizierte Copilot-Taste den Assistenten startet.
- **Image Creator in Microsoft Paint deaktivieren** — Deaktiviert die KI-gestützte Bilderzeugung in Paint.
- **KI-gestützte Bildfüllung in Microsoft Paint deaktivieren** — Deaktiviert KI-gestützte Füllfunktionen in Paint.

Mobile Geräte

Steuert die Integration zwischen Ihrem PC und mobilen Geräten, einschließlich Phone Link und zugehörigen Benachrichtigungen.

Wichtige empfohlene Einstellungen:

- **Phone Link-App deaktivieren** — Deaktiviert die Phone Link-Anwendung.
- **Verbindung des PCs mit mobilen Geräten deaktivieren** — Verhindert PC-zu-Telefon-Konnektivitätsfunktionen.
- **Zugriff auf mobile Geräte deaktivieren** — Blockiert den Zugriff auf mobile Geräte vollständig.
- **Vorschläge zur Nutzung mobiler Geräte mit Windows deaktivieren** — Entfernt Werbebenachrichtigungen über Mobilgeräte-Funktionen.

Verschiedenes

Umfasst zusätzliche datenschutzrelevante Einstellungen, die nicht in andere Kategorien passen, einschließlich Feedback-Erinnerungen, automatische App-Installationen und Netzwerkkonnektivitätsprüfungen.

Wichtige empfohlene Einstellungen:

- **Feedback-Erinnerungen deaktivieren** — Stoppt Microsofts periodische Aufforderungen zur Rückmeldung und Übertragung von Diagnosedaten.
- **Automatische Installation empfohlener Windows Store-Apps deaktivieren** — Verhindert die stille Installation beworbener Apps durch Windows.
- **Tipps, Tricks und Vorschläge bei der Verwendung von Windows deaktivieren** — Unterdrückt Werbe-Popups und Vorschläge im gesamten Betriebssystem.
- **Key Management Service Online-Aktivierung deaktivieren** — Blockiert periodische Aktivierungsüberprüfungen mit Microsoft (nur verwenden, wenn Sie die Auswirkungen verstehen).

Gaming

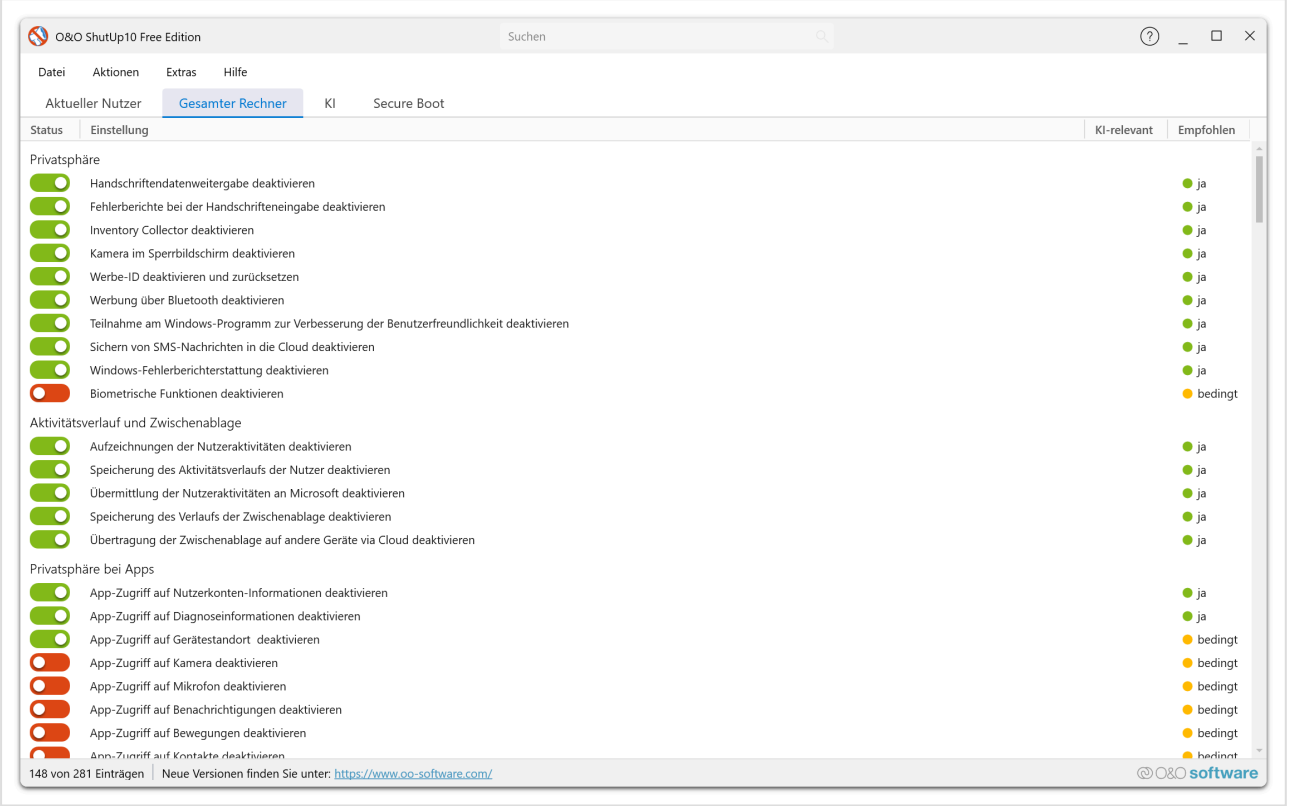
Steuert spielbezogene Funktionen, die Daten sammeln oder unerwünschtes Verhalten verursachen können.

Wichtige empfohlene Einstellungen:

- **Xbox Game Bar und Game DVR deaktivieren** — Deaktiviert die Game Bar, Game DVR und App-Aufnahmefunktionalität und verhindert unerwünschte Microsoft Store-Eingabeaufforderungen.

Telemetriesteuerung

O&O ShutUp10 ermöglicht die Verwaltung der Telemetrie- und Diagnosedaten, die Windows an Microsoft sendet. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Windows sammelt Diagnose- und Nutzungsdaten (Telemetrie) und sendet sie zur Produktverbesserung und Fehlerbehebung an Microsoft. Die Menge der gesammelten Daten hängt von der auf Ihrem System konfigurierten Telemetriestufe ab.

O&O ShutUp10 ermöglicht es Ihnen, die von Windows gesendeten Telemetriedaten zu kontrollieren und zu reduzieren.

Wichtige Telemetrieeinstellungen

Diagnosedatenstufe

Windows bietet mehrere Stufen der Diagnosedatenerfassung an. O&O ShutUp10 ermöglicht es Ihnen, die Stufe auf das erforderliche Minimum zu setzen und so die Menge der mit Microsoft geteilten Daten zu reduzieren.

Maßgeschneiderte Erfahrungen

Microsoft nutzt Diagnosedaten, um personalisierte Tipps, Werbung und Empfehlungen bereitzustellen. Sie können maßgeschneiderte Erfahrungen deaktivieren, um zu verhindern, dass Ihre Diagnosedaten zur Personalisierung verwendet werden.

Feedback-Häufigkeit

Windows fragt regelmäßig nach Feedback. Sie können steuern, wie oft Windows Sie zur Rückmeldung auffordert, oder Feedback-Anfragen vollständig deaktivieren.

Diagnosedaten-Viewer

Windows enthält ein Diagnosedaten-Viewer-Tool. O&O ShutUp10 kann die Erfassungspipeline deaktivieren, die diesen Viewer speist, wenn Sie die Speicherung von Diagnosedaten minimieren möchten.

Fehlerberichterstattung

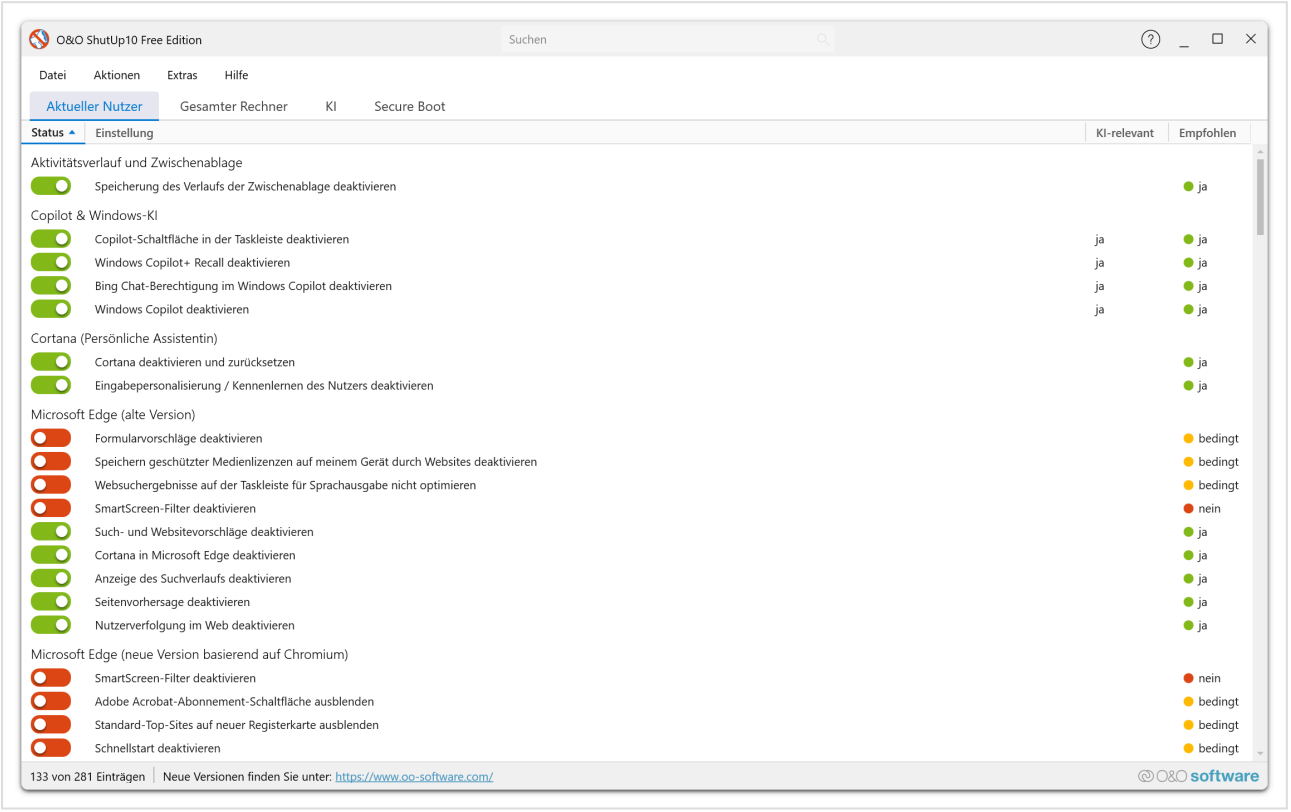
Die Windows-Fehlerberichterstattung sendet Absturz- und Fehlerdaten an Microsoft. Sie können steuern, ob diese Informationen gesammelt und gesendet werden.

Note

Die Reduzierung der Telemetrie auf die niedrigste Stufe kann Microsofts Fähigkeit einschränken, Probleme zu identifizieren und zu beheben, die spezifisch für Ihre Konfiguration sind, verbessert aber erheblich Ihren Datenschutz.

Standortdienste

O&O ShutUp10 gibt Ihnen Kontrolle darüber, wie Windows und seine Apps Ihre Standortdaten nutzen. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Windows nutzt Standortdienste, um standortbezogene Funktionen wie Wetter, Karten und standortbasierte Erinnerungen bereitzustellen. Diese Dienste sind zwar nützlich, übertragen aber auch Ihren physischen Standort an Microsoft und Drittanbieter-Apps.

Was Sie kontrollieren können

Systemweiter Standortzugriff

Deaktivieren Sie den Standortzugriff für das gesamte System. Wenn deaktiviert, können keine Apps oder Dienste auf den Standort Ihres Geräts zugreifen.

App-spezifische Standortberechtigungen

Steuern Sie, welche einzelnen Apps auf Ihre Standortdaten zugreifen dürfen.

Standortverlauf

Windows speichert einen Verlauf der Standorte, an denen sich Ihr Gerät befunden hat. O&O ShutUp10 ermöglicht es Ihnen, die Erfassung des Standortverlaufs zu deaktivieren.

Geofencing

Einige Apps verwenden Geofencing, um Aktionen auszulösen, wenn Sie einen bestimmten Bereich betreten oder verlassen. Sie können diese Funktionalität deaktivieren.

Standortbasierte Werbung

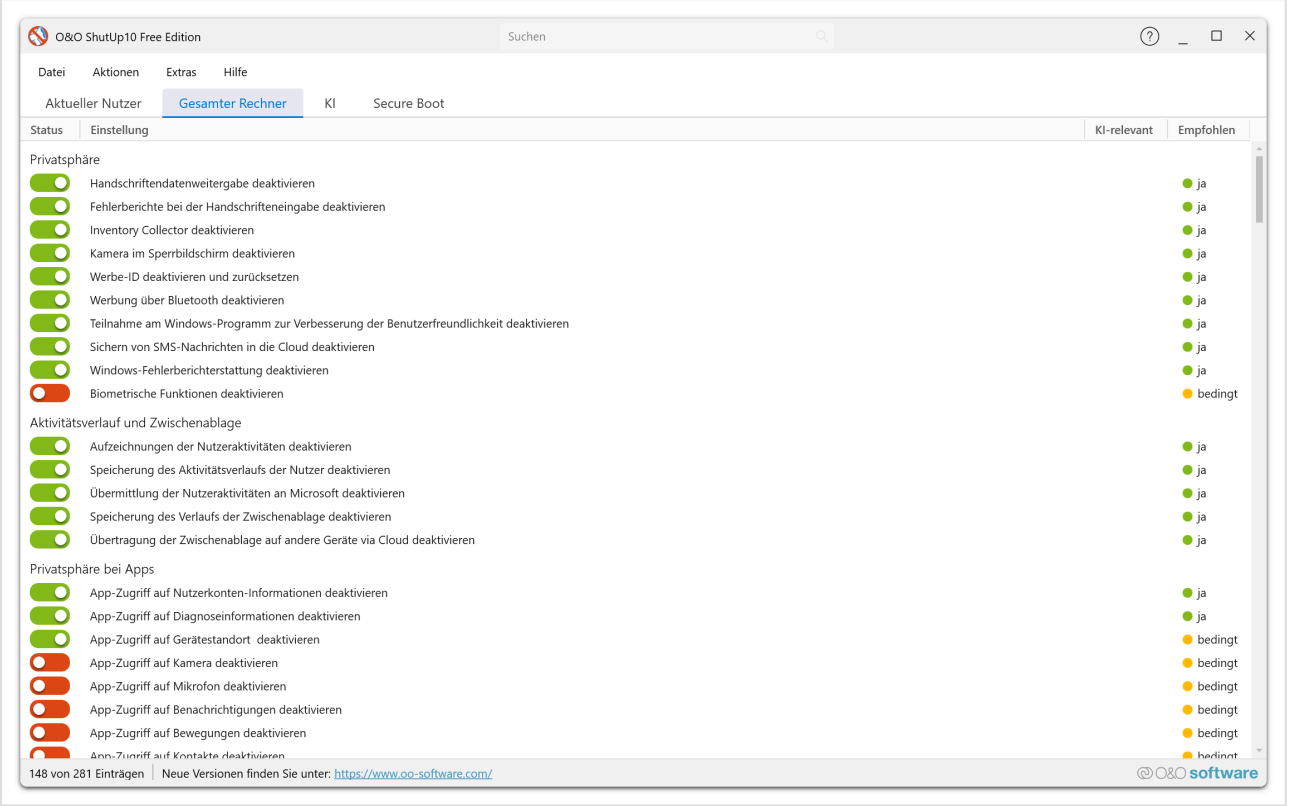
Werbenetzwerke können Ihren Standort nutzen, um gezielte Werbung zu schalten. Sie können verhindern, dass Ihre Standortdaten für Werbezwecke verwendet werden.

Tip

Wenn Sie keine standortbasierten Apps nutzen (Karten, Wetter-Widgets usw.), wird die vollständige Deaktivierung der Standortdienste für maximalen Datenschutz empfohlen.

Windows Update-Einstellungen

O&O ShutUp10 bietet Kontrolle über das Verhalten von Windows Update. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Windows Update ist für Sicherheit und Stabilität unverzichtbar, enthält aber auch Funktionen, die Ihren Datenschutz beeinträchtigen können, wie Peer-to-Peer-Update-Freigabe und automatische Treiberdownloads.

Was Sie kontrollieren können

Update-Bereitstellungsoptimierung

Windows kann heruntergeladene Updates mit anderen PCs in Ihrem lokalen Netzwerk oder über das Internet teilen (Peer-to-Peer-Bereitstellung). O&O ShutUp10 ermöglicht es Ihnen, diese Funktion zu deaktivieren oder auf Ihr lokales Netzwerk zu beschränken.

Automatische Treiberupdates

Windows Update kann automatisch Treiber von Microsoft herunterladen und installieren. Sie können steuern, ob dies geschieht, oder Treiberupdates manuell verwalten.

Automatische App-Updates

Der Microsoft Store aktualisiert Apps automatisch im Hintergrund. Sie können dieses Verhalten über O&O ShutUp10 steuern.

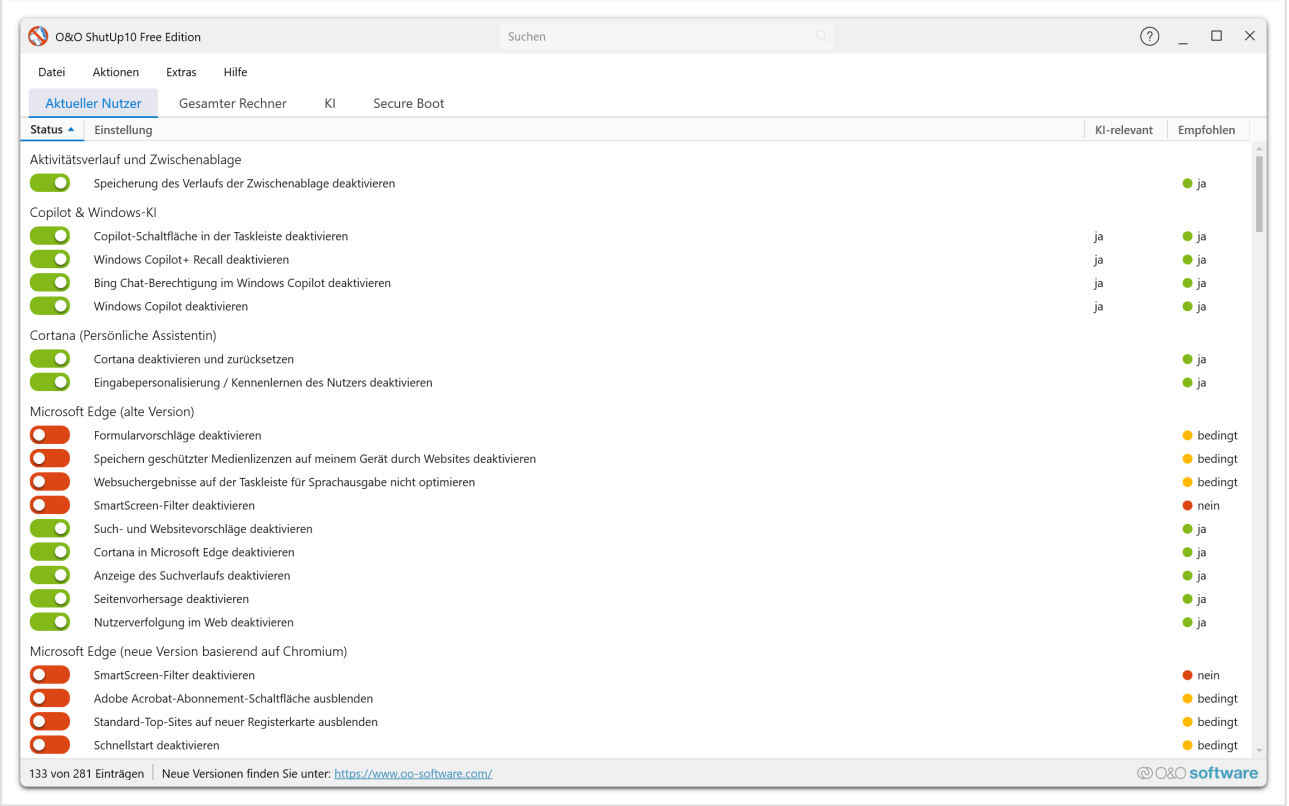
Automatische Windows-Updates

Steuern Sie, wie Windows mit Update-Downloads und Installationszeitplänen umgeht.

> **Caution**
>
> Das Deaktivieren von Windows Update-Funktionen kann Ihr System ohne kritische Sicherheitspatches lassen. Passen Sie diese Einstellungen nur an, wenn Sie eine alternative Update-Strategie haben.

Cortana & Suche-Einstellungen

O&O ShutUp10 bietet Kontrolle über das Verhalten von Cortana und der Windows-Suche. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Cortana und die Windows-Suche können Suchanfragen, Sprachdaten und Nutzungsmuster an Microsoft senden. O&O ShutUp10 ermöglicht es Ihnen, diese Funktionen für mehr Datenschutz einzuschränken oder zu deaktivieren.

Was Sie kontrollieren können

Websuche im Startmenü

Standardmäßig sendet Windows Ihre Startmenü-Suchanfragen an Bing. Sie können Websuchergebnisse deaktivieren, um Ihre Suchen lokal auf Ihrem Gerät zu halten.

Cortana-Sprachaktivierung

Cortana kann auf Sprachbefehle hören. Sie können die Sprachaktivierung deaktivieren, um jegliche Verarbeitung von Umgebungsaudio zu verhindern.

Suchverlauf

Windows speichert Ihren Suchverlauf, um zukünftige Ergebnisse zu verbessern. Sie können die Erfassung des Suchverlaufs deaktivieren.

Cloud-Suche

Die Windows-Suche kann Ergebnisse aus Ihren Cloud-Diensten (OneDrive, Outlook usw.) einbeziehen. Sie können die Suche auf lokale Inhalte beschränken.

Suchindizierung

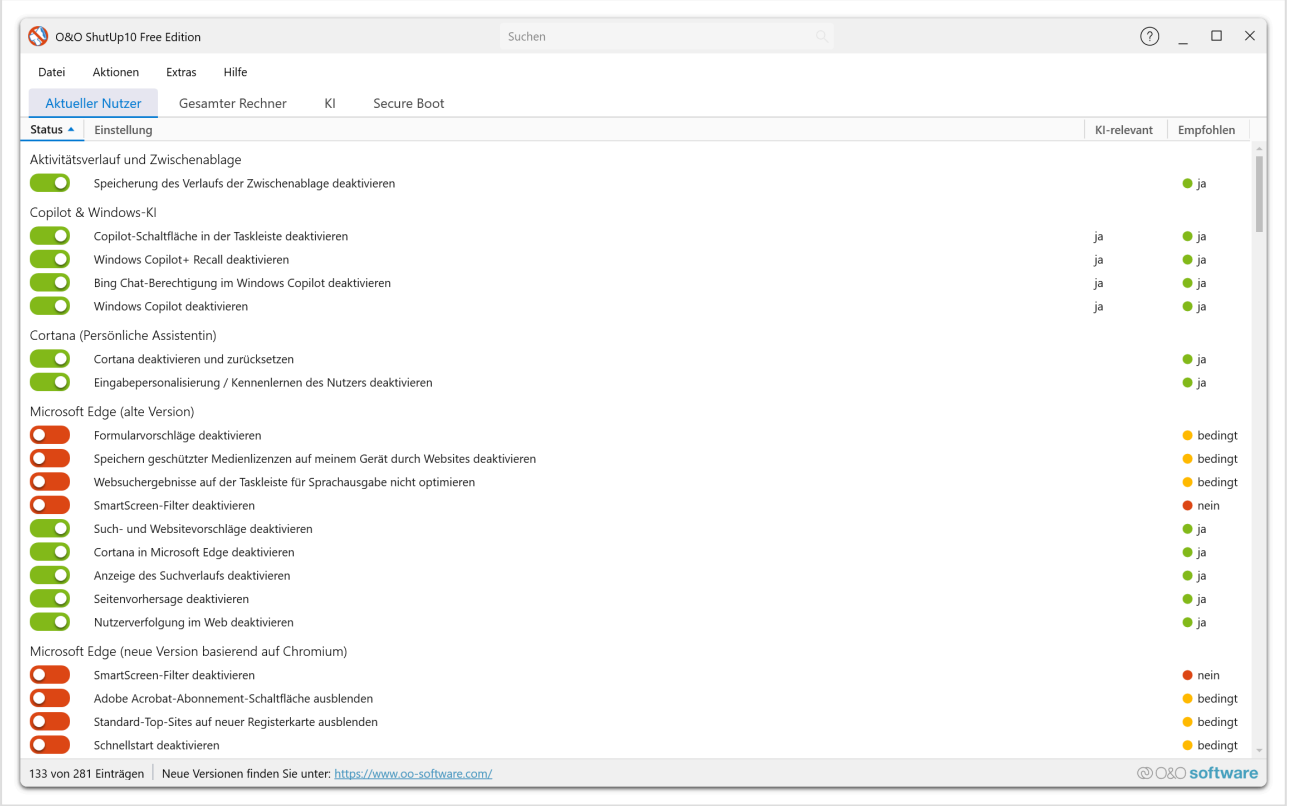
Steuern Sie, wie Windows Dateien und Inhalte für die Suche indiziert, einschließlich welcher Speicherorte indiziert werden und welche Inhaltstypen enthalten sind.

Tip

Die Deaktivierung der Websuche im Startmenü ist eine der beliebtesten Datenschutzanpassungen, da sie verhindert, dass jede lokale Suche an Microsofts Server gesendet wird.

App-Berechtigungen

O&O ShutUp10 ermöglicht die Verwaltung der Berechtigungen, auf die Windows-Apps zugreifen können. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Windows gewährt Apps Zugriff auf verschiedene Systemressourcen wie Ihre Kamera, Ihr Mikrofon, Kontakte, Kalender und mehr. O&O ShutUp10 ermöglicht die zentrale Verwaltung dieser Berechtigungen, anstatt jede einzeln über die Windows-Einstellungen zu konfigurieren.

Was Sie kontrollieren können

Kamerazugriff

Steuern Sie, welche Apps auf die Kamera Ihres Geräts zugreifen können. Sie können den Kamerazugriff systemweit deaktivieren oder pro App verwalten.

Mikrofonzugriff

Steuern Sie, welche Apps auf Ihr Mikrofon zugreifen können. Dies ist besonders wichtig für den Datenschutz, da der Mikrofonzugriff zum Abhören der Umgebung genutzt werden kann.

Kontaktzugriff

Verwalten Sie, welche Apps Ihre Kontaktliste lesen können.

Kalenderzugriff

Steuern Sie, welche Apps auf Ihre Kalendereinträge zugreifen können.

Anrufverlauf

Verwalten Sie den Zugriff auf Ihren Anrufverlauf, falls zutreffend.

E-Mail-Zugriff

Steuern Sie, welche Apps auf Ihre E-Mail-Konten und Nachrichten zugreifen können.

Nachrichtenzugriff

Verwalten Sie, welche Apps Textnachrichten lesen oder senden können.

Benachrichtigungszugriff

Steuern Sie, welche Apps auf Ihre Benachrichtigungen zugreifen können.

Kontoinformationen

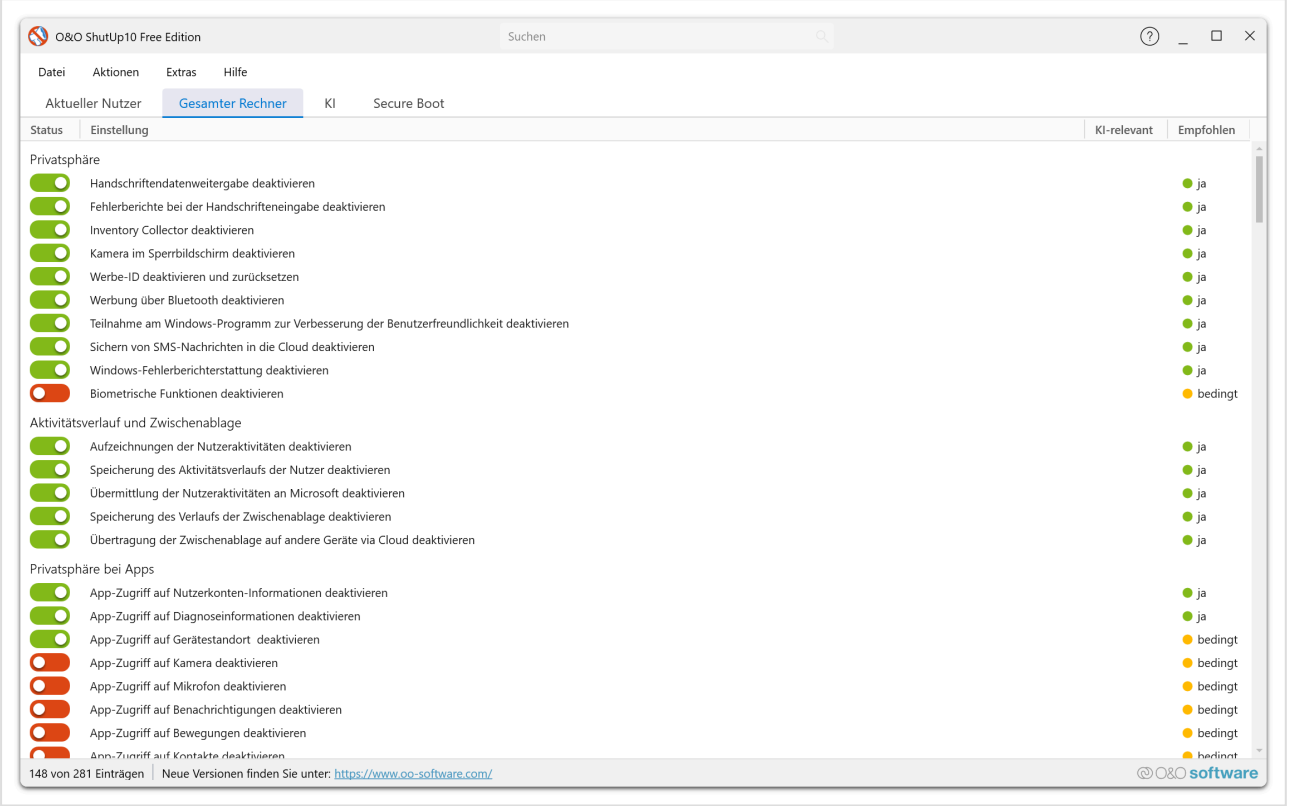
Verwalten Sie, welche Apps auf Ihren Kontonamen, Ihr Profilbild und andere Profilinformationen zugreifen können.

Note

Die Einschränkung von App-Berechtigungen kann dazu führen, dass einige Apps Funktionalität verlieren. Überprüfen Sie jede Berechtigung sorgfältig, bevor Sie sie deaktivieren.

Windows Explorer & Werbung

O&O ShutUp10 bietet Kontrolle über das Verhalten des Windows Explorers und werbebezogene Einstellungen. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Windows Explorer und die Windows-Shell enthalten mehrere Funktionen, die Werbung, Vorschläge und Werbeinhalte anzeigen. O&O ShutUp10 ermöglicht es Ihnen, diese zu deaktivieren, um eine sauberere, ablenkungsfreie Erfahrung zu schaffen.

Was Sie kontrollieren können

Synchronisierungsanbieter-Benachrichtigungen

Windows Explorer kann Benachrichtigungen von Synchronisierungsanbietern wie OneDrive anzeigen. Sie können diese Benachrichtigungen deaktivieren.

Tipps und Vorschläge

Windows kann Tipps zu Windows-Funktionen und Vorschläge für Apps anzeigen. Sie können diese Eingabeaufforderungen deaktivieren.

Startmenü-Vorschläge

Das Startmenü kann App-Vorschläge anzeigen (im Wesentlichen Werbung für Microsoft Store-Apps). O&O ShutUp10 ermöglicht es Ihnen, diese zu deaktivieren.

Sperrbildschirm-Werbung

Der Windows-Sperrbildschirm kann Tipps, Tricks und Werbung anzeigen. Sie können den Sperrbildschirm so konfigurieren, dass nur Ihr gewähltes Hintergrundbild angezeigt wird.

Zeitleiste und Aktivitätsverlauf

Die Windows-Zeitleiste verfolgt Ihre Aktivitäten über Apps und Geräte hinweg. Sie können die Erfassung des Aktivitätsverlaufs und die Zeitleistenfunktion deaktivieren.

OneDrive-Integration

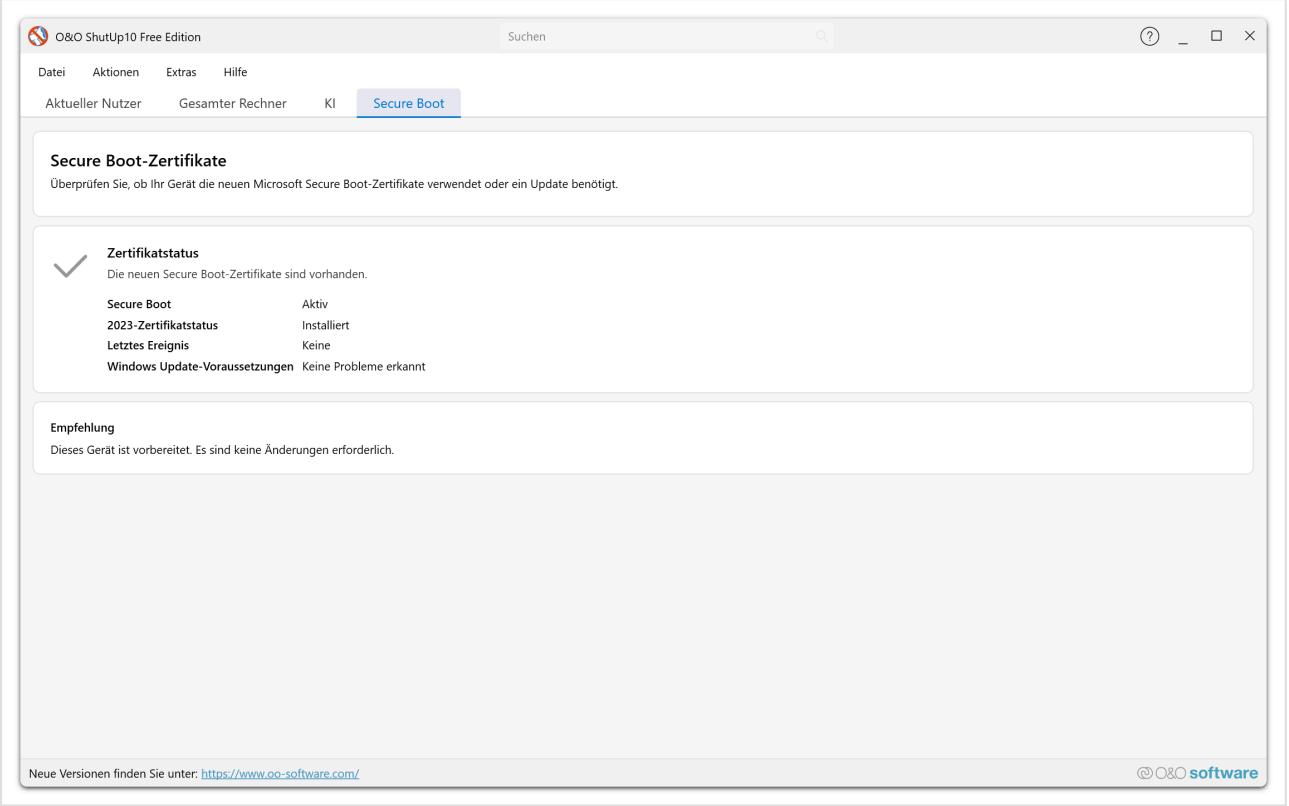
Steuern Sie den Grad der OneDrive-Integration im Windows Explorer, einschließlich Auto-Start und Werbeinhalte.

Tip

Die Deaktivierung werbebezogener Einstellungen im Windows Explorer wird für alle Benutzer empfohlen und hat keine negativen Auswirkungen auf die Funktionalität.

Sicherheitseinstellungen

O&O ShutUp10 umfasst die Steuerung bestimmter sicherheitsbezogener Windows-Einstellungen. Diese Einstellungen sind in der Free und Premium Edition verfügbar.



Überblick

Obwohl O&O ShutUp10 in erster Linie ein Datenschutz-Tool ist, überschneiden sich einige Windows-Sicherheitsfunktionen mit dem Datenschutz. Beispielsweise sendet die cloudbasierte Malware-Erkennung Dateiinformationen an Microsoft, und bestimmte Sicherheitsfunktionen übertragen Telemetriedaten. O&O ShutUp10 ermöglicht die Feinabstimmung dieser Einstellungen.

Was Sie kontrollieren können

Windows Defender Cloud-Schutz

Windows Defender kann Dateiproben und Erkennungsinformationen zur erweiterten Erkennung an Microsofts Cloud senden. Sie können diese Funktion steuern, wenn Sie Dateiinformationen lieber lokal behalten möchten.

Automatische Probenübermittlung

Windows Defender kann verdächtige Dateiproben automatisch zur Analyse an Microsoft übermitteln. O&O ShutUp10 ermöglicht es Ihnen, diese automatische Übermittlung zu deaktivieren.

Windows-Sicherheitsbenachrichtigungen

Steuern Sie die von Windows-Sicherheit (ehemals Windows Defender Security Center) angezeigten Benachrichtigungen.

Benutzerkontensteuerung (UAC)

Feinabstimmung des UAC-Verhaltens, einschließlich Benachrichtigungsstufen und Admin-Genehmigungsmodus.

Caution

Die Anpassung von Sicherheitseinstellungen kann die Wirksamkeit von Windows Defender oder anderen Sicherheitsfunktionen verringern. Ändern Sie diese Einstellungen nur, wenn Sie alternative Sicherheitsmaßnahmen getroffen haben.

Häufig gestellte Fragen

Diese FAQ behandelt die häufigsten Fragen zu O&O ShutUp10, Windows-Datenschutzeinstellungen und bewährte Praktiken für die Verwaltung des Datenschutzes unter Windows 10 und Windows 11.

Allgemeine Fragen

Was ist O&O ShutUp10?

O&O ShutUp10 ist ein kostenloses Antispionage-Tool, entwickelt von O&O Software GmbH für Windows 10 und Windows 11. Es bietet eine einzige, benutzerfreundliche Oberfläche zur Verwaltung von fast 300 datenschutzrelevanten Einstellungen, die ansonsten über die Windows-Einstellungs-App, Gruppenrichtlinien und die Windows-Registry verteilt sind. Das Tool ermöglicht es Ihnen zu entscheiden, welche Telemetrie-, Tracking- und Datenfreigabefunktionen deaktiviert werden sollen — ohne tiefes technisches Wissen zu erfordern.

Eine vollständige Übersicht finden Sie in der Einführung.

Ist O&O ShutUp10 wirklich kostenlos?

Ja. Die **Free Edition** von O&O ShutUp10 ist für den privaten und kommerziellen Gebrauch völlig kostenlos. Es ist eine portable Anwendung — keine Installation erforderlich. Sie laden einfach die Anwendung herunter und führen sie aus.

O&O Software bietet auch eine **Premium Edition** mit zusätzlichen Funktionen wie automatischem Hintergrundschutz und einer Client/Service-Architektur an. Die Premium Edition ist ein kostenpflichtiges Produkt für professionelle und Unternehmensumgebungen.

Funktioniert O&O ShutUp10 sowohl unter Windows 10 als auch unter Windows 11?

Ja. O&O ShutUp10 unterstützt sowohl Windows 10 als auch Windows 11. Das Tool wird regelmäßig aktualisiert, um neue datenschutzrelevante Einstellungen abzudecken, die Microsoft in beiden Betriebssystemen einführt. Einige Einstellungen sind versionsspezifisch und erscheinen nur bei Ausführung auf der jeweiligen Windows-Version.

Ist O&O ShutUp10 sicher zu verwenden? Kann es mein System beschädigen?

O&O ShutUp10 ändert Windows-Datenschutzeinstellungen über dokumentierte Registry-Schlüssel und Gruppenrichtlinieneinträge — die gleichen Mechanismen, die Windows selbst und Systemadministratoren verwenden. Es löscht keine Systemdateien, ändert keine Boot-Konfigurationen und verändert keine Kernkomponenten des Betriebssystems.

Jede von O&O ShutUp10 vorgenommene Änderung ist vollständig reversibel. Das Tool erstellt einen Systemwiederherstellungspunkt vor dem Anwenden von Änderungen (falls aktiviert), und Sie können jede einzelne Einstellung rückgängig machen oder alle Standards aus der Anwendung heraus wiederherstellen.

> **Caution**
>
> Das Deaktivieren bestimmter Einstellungen (insbesondere solcher, die als **Nicht empfohlen** markiert sind) kann die Systemfunktionalität beeinträchtigen. Überprüfen Sie immer die Empfehlungsstufe und Beschreibung jeder Einstellung, bevor Sie sie anwenden.

Installation und Systemanforderungen

Erfordert O&O ShutUp10 eine Installation?

Die **Free Edition** erfordert keine Installation. Es ist eine portable Anwendung — laden Sie sie herunter, führen Sie sie aus, und sie funktioniert sofort. Keine Dateien verbleiben auf Ihrem System, nachdem Sie sie schließen (außer den Datenschutzeinstellungsänderungen, die Sie angewendet haben).

Die **Premium Edition** verwendet eine Client/Service-Architektur und erfordert eine Installation, da der Hintergrunddienst bei Windows registriert werden muss, um automatischen, proaktiven Schutz zu bieten.

Erfordert O&O ShutUp10 Administratorrechte?

Ja. Da O&O ShutUp10 Registry-Schlüssel und Gruppenrichtlinieneinstellungen auf Systemebene ändert, sind **Administratorrechte** zum Ausführen erforderlich. Die Free Edition fordert bei jedem Start eine Erhöhung (UAC) an. Der Hintergrunddienst der Premium Edition läuft automatisch mit den erforderlichen Berechtigungen, sodass Endbenutzer keinen Administratorzugang auf ihren Rechnern benötigen.

Verwendung von O&O ShutUp10

Was bedeuten die farbigen Umschalter?

O&O ShutUp10 verwendet ein Ampel-Farbschema für seine Umschalter:

Farbe	Bedeutung
Grün (ein)	Der Datenschutz ist **aktiv** — die entsprechende Windows-Funktion ist deaktiviert.
Rot (aus)	Der Datenschutz ist **inaktiv** — die Windows-Funktion läuft mit ihrem Standardverhalten.

Ein **grüner** Umschalter bedeutet, dass das Tool diese bestimmte Tracking- oder Datenfreigabefunktion blockiert hat, während ein **roter** Umschalter bedeutet, dass Windows für diese Einstellung normal arbeitet.

Was sind die Empfehlungsstufen und welche Einstellungen sollte ich anwenden?

Jede Einstellung in O&O ShutUp10 enthält eine Empfehlungsstufe:

Stufe	Beschreibung
Empfohlen	Sicher für die meisten Benutzer. Das Deaktivieren dieser Funktionen hat keine negativen Auswirkungen auf die Kernfunktionalität von Windows.
Eingeschränkt	Grundsätzlich sicher, kann aber bestimmte Personalisierungs- oder Komfortfunktionen beeinträchtigen (z.B. Cortana, Aktivitätsverlauf).
Nicht empfohlen	Kann wichtige Funktionalität wie Windows Update-Bereitstellung, Windows Defender oder Systemaktivierung beeinträchtigen. Nur anwenden, wenn Sie die Konsequenzen vollständig verstehen.

> **Tip**
>
> Wenn Sie unsicher sind, wo Sie anfangen sollen, wenden Sie zunächst nur die **Empfohlenen** Einstellungen an. Sie können einzelne Einstellungen jederzeit überprüfen und anpassen.

Eine vollständige Beschreibung der Einstellungskategorien finden Sie in der Übersicht der Datenschutzeinstellungen.

Kann ich alle empfohlenen Einstellungen auf einmal anwenden?

Ja. O&O ShutUp10 bietet ein **Aktionen**-Menü, mit dem Sie alle Einstellungen einer bestimmten Empfehlungsstufe in einem Schritt anwenden können. Sie können wählen, ob Sie alle **Empfohlenen** Einstellungen, alle **Empfohlenen und Eingeschränkten** Einstellungen oder alle Einstellungen unabhängig von der Stufe anwenden möchten. Dies ist der schnellste Weg, Ihr System zu konfigurieren.

Was sind Profile und wie verwende ich sie?

Profile ermöglichen es Ihnen, Ihre aktuelle Konfiguration (den Status aller Umschalter) in einer Datei zu speichern und später wieder zu laden. Dies ist nützlich für:

- **Sichern** Ihrer bevorzugten Einstellungen, bevor Sie Änderungen vornehmen.
- **Teilen** einer konsistenten Konfiguration über mehrere Computer hinweg.
- **Wiederherstellen** Ihres bevorzugten Status, nachdem ein Windows-Update Ihre Datenschutzeinstellungen zurückgesetzt hat.

Sie können ein Profil über **Datei → Einstellungen exportieren** exportieren und mit **Datei → Einstellungen importieren** importieren. Profildateien verwenden das `.cfg`-Dateiformat.

Weitere Details finden Sie in der Dokumentation zu Profile & Export.

Empfehlungsstufen und Profile

Was ist der Unterschied zwischen „Empfohlen", „Eingeschränkt" und „Nicht empfohlen"?

Diese Stufen geben die potenzielle Auswirkung der Deaktivierung einer Windows-Funktion an:

- **Empfohlene** Einstellungen deaktivieren Telemetrie- und Tracking-Funktionen, die die meisten Benutzer nicht benötigen. Das Anwenden dieser Einstellungen verbessert Ihren Datenschutz ohne spürbaren Einfluss auf die tägliche Nutzung.
- **Eingeschränkte** Einstellungen deaktivieren Funktionen, auf die einige Benutzer möglicherweise angewiesen sind, wie Cortana, Websuche-Integration oder Synchronisierung des Aktivitätsverlaufs. Das Deaktivieren ist sicher, kann aber Ihren Arbeitsablauf ändern.
- **Nicht empfohlene** Einstellungen steuern Funktionen, die für die Systemstabilität oder -sicherheit wichtig sind, wie Windows Update Peer-to-Peer-Bereitstellung, Windows Defender-Telemetrie oder Systemaktivierung. Deaktivieren Sie diese nur, wenn Sie einen bestimmten Grund haben und die möglichen Nebenwirkungen verstehen.

Wird das Anwenden von „Nicht empfohlenen" Einstellungen meinen Computer beschädigen?

Das Anwenden von „Nicht empfohlenen" Einstellungen wird Ihren Computer nicht dauerhaft beschädigen, kann aber unerwünschtes Verhalten verursachen. Beispiele umfassen:

- **Windows Update-Probleme** — Das Deaktivieren der Update-Bereitstellungsoptimierung kann Downloads verlangsamen oder verhindern.
- **Reduzierte Sicherheit** — Das Deaktivieren der Defender-Probenübermittlung oder SpyNet-Mitgliedschaft reduziert die Wirksamkeit der Echtzeit-Bedrohungserkennung.
- **Aktivierungsprobleme** — Das Deaktivieren der KMS-Online-Aktivierung kann dazu führen, dass die Windows-Aktivierung auf volumenlizenzierten Systemen fehlschlägt.

Alle Änderungen sind reversibel. Wenn Sie nach dem Anwenden einer Einstellung Probleme bemerken, schalten Sie sie einfach in ihren ursprünglichen Zustand zurück oder verwenden Sie die **Rückgängig**-Funktion.

Änderungen rückgängig machen und Standards wiederherstellen

Wie mache ich Änderungen rückgängig, die von O&O ShutUp10 vorgenommen wurden?

Es gibt mehrere Möglichkeiten, Änderungen rückgängig zu machen:

1. **Einzelne Einstellungen umschalten** — Klicken Sie auf einen grünen Umschalter, um ihn auf Rot (aus) zu setzen und den Windows-Standard für diese Einstellung wiederherzustellen.
2. **Alle Änderungen rückgängig machen** — Verwenden Sie das **Aktionen**-Menü und wählen Sie **Alle Änderungen rückgängig machen**, um jede Einstellung auf ihren Windows-Standard zurückzusetzen.
3. **Gespeichertes Profil importieren** — Wenn Sie Ihre Einstellungen vor Änderungen exportiert haben, importieren Sie das gespeicherte Profil, um Ihre vorherige Konfiguration wiederherzustellen.
4. **Systemwiederherstellung** — Wenn Sie einen Systemwiederherstellungspunkt erstellt haben, bevor Sie Änderungen angewendet haben (O&O ShutUp10 kann Sie dazu auffordern), können Sie die Windows-Systemwiederherstellung verwenden, um Ihr gesamtes System auf den früheren Zustand zurückzusetzen.

Erstellt O&O ShutUp10 automatisch einen Systemwiederherstellungspunkt?

O&O ShutUp10 bietet an, einen Systemwiederherstellungspunkt zu erstellen, bevor Änderungen angewendet werden. Wenn Sie zum ersten Mal Einstellungen anwenden, fordert das Tool Sie auf, einen zu erstellen. Es wird dringend empfohlen, diese Aufforderung zu akzeptieren, da sie ein Sicherheitsnetz bietet, mit dem Sie alle Änderungen über die Standard-Windows-Systemwiederherstellungsfunktion zurücksetzen können.

Windows-Updates und Kompatibilität

Wird Windows Update meine Datenschutzeinstellungen zurücksetzen?

Ja, dies ist ein bekanntes und häufiges Problem. Große Windows-Feature-Updates (z.B. Upgrade von Windows 10 22H2 auf Windows 11 23H2 oder Anwendung jährlicher Feature-Updates) können einige oder alle der von Ihnen geänderten Datenschutzeinstellungen zurücksetzen. Microsofts Update-Prozess kann Standard-Telemetrie- und -Tracking-Konfigurationen wiederherstellen.

Was nach einem großen Update zu tun ist:

1. Führen Sie O&O ShutUp10 erneut aus und überprüfen Sie Ihre Einstellungen — alle zurückgesetzten Umschalter erscheinen rot.
2. Wenden Sie Ihre bevorzugten Einstellungen manuell erneut an oder importieren Sie ein zuvor gespeichertes Profil.
3. Die **Premium Edition** erledigt dies automatisch: Ihr Hintergrunddienst erkennt, wenn Einstellungen zurückgesetzt wurden, und wendet Ihre bevorzugte Konfiguration ohne manuellen Eingriff erneut an.

Ist es sicher, O&O ShutUp10 zusammen mit Windows Update zu verwenden?

Ja. O&O ShutUp10 stört den Windows Update-Mechanismus selbst nicht. Sicherheitsupdates, kumulative Updates und Treiberupdates werden weiterhin normal heruntergeladen und installiert.

Wenn Sie jedoch bestimmte Update-bezogene Einstellungen deaktivieren (wie **Peer-to-Peer-Update-Bereitstellung** oder **optionale/Vorschau-Updates**), ändern sich diese Verhaltensweisen wie beabsichtigt. Kritische Sicherheitsupdates werden durch keine der empfohlenen Einstellungen beeinträchtigt.

Windows Defender und Sicherheit

Deaktiviert O&O ShutUp10 Windows Defender?

O&O ShutUp10 deaktiviert Windows Defender standardmäßig **nicht**. Die Defender-bezogenen Einstellungen im Tool steuern **Datenfreigabeverhalten** — z.B. ob Defender Dateiproben zur Cloud-Analyse an Microsoft sendet oder am Microsoft SpyNet-Telemetrienetzwerk teilnimmt.

Das Deaktivieren dieser Datenfreigabefunktionen reduziert die an Microsoft gesendeten Informationen, kann aber die Wirksamkeit der cloudbasierten Bedrohungserkennung von Defender leicht verringern. Die Kern-Antivirus-Engine, der Echtzeitschutz und das lokale signaturbasierte Scannen bleiben voll funktionsfähig.

> **Caution**
>
> Deaktivieren Sie Windows Defender nicht vollständig, es sei denn, Sie haben eine alternative, regelmäßig aktualisierte Antivirenlösung installiert und aktiv.

Kann ich O&O ShutUp10 zusammen mit Antivirus-Software von Drittanbietern verwenden?

Ja. O&O ShutUp10 verwaltet Datenschutzeinstellungen auf Betriebssystemebene und steht nicht in Konflikt mit Antivirus-Software von Drittanbietern. Wenn Sie bereits eine Drittanbieterlösung verwenden (die Windows Defender typischerweise automatisch deaktiviert), können Sie alle Defender-bezogenen Datenschutzeinstellungen in O&O ShutUp10 sicher anwenden.

Windows-Datenschutzeinstellungen

Was ist Windows-Telemetrie und warum sollte mich das interessieren?

Windows-Telemetrie bezeichnet die Diagnose- und Nutzungsdaten, die Windows sammelt und an Microsoft sendet. Diese Daten können umfassen:

- **Hardware- und Softwareinventar** — Details über Ihr Gerät, installierte Anwendungen und Treiber.
- **Nutzungsmuster** — Wie Sie Windows-Funktionen, Apps und Dienste verwenden.
- **Absturzberichte und Fehlerprotokolle** — Informationen über Anwendungs- und Systemfehler, die Speicherauszüge mit persönlichen Daten enthalten können.
- **Browser- und Suchdaten** — Abfragen, die in das Startmenü, Cortana oder Edge eingegeben werden.

Microsoft nutzt diese Daten zur Produktverbesserung und Personalisierung, aber viele Benutzer und Organisationen bevorzugen es, diese Datenerfassung aus Gründen des Datenschutzes, der Compliance oder der Sicherheit zu minimieren oder zu eliminieren.

O&O ShutUp10 ermöglicht die Kontrolle der Telemetrie auf granularer Ebene. Das Anwenden der **Empfohlenen** Telemetrieeinstellungen reduziert die Datenerfassung erheblich, ohne die Systemfunktionalität zu beeinträchtigen.

Details zu den Telemetrieeinstellungen finden Sie in der Dokumentation zur Telemetriesteuerung.

Was ist der Unterschied zwischen Windows 10 und Windows 11 Datenschutzeinstellungen?

Windows 11 führte mehrere neue datenschutzrelevante Funktionen ein und erweiterte bestehende:

- **Widgets und Nachrichten-Feed** — Windows 11 fügte ein Widget-Panel hinzu, das mit Microsoft-Servern kommuniziert. O&O ShutUp10 enthält Einstellungen, um dies zu deaktivieren.
- **Microsoft Copilot** — Windows 11 führte einen KI-Assistenten (Copilot) mit eigener Datenerfassung ein. O&O ShutUp10 bietet Einstellungen zum Deaktivieren von Copilot und seiner Tastenkombination.
- **Erweiterte Telemetrie** — Windows 11 erweiterte bestimmte Telemetriekategorien. O&O ShutUp10 deckt diese zusätzlichen Datenpunkte ab.
- **Snap-Layouts und Desktop-Organisation** — Einige neue UI-Funktionen haben Telemetriekomponenten, die gesteuert werden können.
- **Phone Link-Integration** — Tiefere Mobilgeräte-Integration in Windows 11 bringt zusätzliche Datenschutzaspekte mit sich.

O&O ShutUp10 erkennt automatisch Ihre Windows-Version und zeigt nur die für Ihr System relevanten Einstellungen an. Einstellungen, die nur für Windows 11 gelten, erscheinen nicht auf einem Windows 10-Rechner und umgekehrt.

Was passiert, wenn ich Standortdienste deaktiviere?

Das Deaktivieren der Standortdienste verhindert, dass Windows und Apps über GPS, Wi-Fi-Positionsbestimmung oder Gerätesensoren auf Ihren physischen Standort zugreifen. Das bedeutet:

- **Wetter-Apps** erkennen Ihren Standort nicht automatisch (Sie können einen Standort weiterhin manuell festlegen).
- **Karten und Navigation** können Ihre Position nicht bestimmen.
- **Mein Gerät finden** funktioniert nicht.
- **Standortbasierte Erinnerungen** (z.B. in Cortana) funktionieren nicht.
- **Automatische Bildschirmdrehung** auf Tablets kann beeinträchtigt sein, wenn auch der Sensorzugriff deaktiviert ist.

Für die meisten Desktop-Benutzer hat das Deaktivieren der Standortdienste keinen praktischen Nachteil. Tablet- und Laptop-Benutzer, die auf GPS oder standortbasierte Funktionen angewiesen sind, sollten in Betracht ziehen, diese Einstellung aktiviert zu lassen.

Details zu den einzelnen Standorteinstellungen finden Sie in der Dokumentation zu Standortdienste.

Sollte ich Cortana und die Websuche im Startmenü deaktivieren?

Das Deaktivieren von Cortana und der Websuche verhindert, dass in das Startmenü eingegebene Suchanfragen an Microsofts Bing-Server gesendet werden. Stattdessen liefern Suchen nur lokale Ergebnisse (installierte Apps, Dateien und Einstellungen).

Dies ist eine der am häufigsten angewendeten Datenschutzeinstellungen und ist in O&O ShutUp10 als **Empfohlen** eingestuft. Die meisten Benutzer stellen fest, dass die rein lokale Suche schneller ist und relevantere Ergebnisse liefert, und sie eliminiert vollständig die Übertragung von Suchanfragen an Microsoft.

Alle zugehörigen Einstellungen finden Sie in der Dokumentation zu Cortana & Suche.

Fehlerbehebung

Eine Einstellung wird immer wieder auf ihren ursprünglichen Zustand zurückgesetzt. Was kann ich tun?

Einige Windows-Einstellungen können zurückgesetzt werden durch:

- **Windows Update** — Feature-Updates und manchmal kumulative Updates können Standard-Datenschutzeinstellungen wiederherstellen.
- **Gruppenrichtlinie** — In domänenverbundenen (Unternehmens-) Umgebungen kann die Gruppenrichtlinie lokale Einstellungen überschreiben.
- **Geplante Aufgaben** — Bestimmte geplante Windows-Aufgaben können regelmäßig Telemetriefunktionen wieder aktivieren.

Lösungen:

1. Führen Sie O&O ShutUp10 nach jedem größeren Windows-Update erneut aus und wenden Sie Ihre Einstellungen erneut an.
2. Exportieren Sie Ihre Einstellungen als Profil, damit Sie sie schnell erneut importieren können.
3. Erwägen Sie die **Premium Edition**, die automatisch erkennt und Einstellungen erneut anwendet, die zurückgesetzt wurden.

O&O ShutUp10 zeigt eine Einstellung als „nicht verfügbar" oder ausgegraut an. Warum?

Eine Einstellung kann aus mehreren Gründen nicht verfügbar sein:

- **Windows-Versionskonflikt** — Die Einstellung gilt nur für eine Windows-Version, die Sie nicht verwenden (z.B. eine nur für Windows 11 geltende Einstellung auf einem Windows 10-Rechner).
- **Editionsbeschränkung** — Einige Einstellungen gelten nur für bestimmte Windows-Editionen (z.B. Pro, Enterprise oder Education), da sie auf Gruppenrichtlinienfunktionen angewiesen sind, die in Home-Editionen nicht verfügbar sind.
- **Funktion nicht installiert** — Die Windows-Funktion, die die Einstellung steuert, ist auf Ihrem System nicht installiert (z.B. Microsoft Office-Einstellungen, wenn Office nicht installiert ist).

Dieses Verhalten ist erwartet und weist nicht auf ein Problem mit O&O ShutUp10 hin.

Ich habe Einstellungen angewendet und jetzt funktioniert etwas auf meinem System nicht korrekt. Was soll ich tun?

1. **Identifizieren Sie die betroffene Funktionalität** — Bestimmen Sie, was nicht mehr funktioniert (z.B. Startmenü-Suche, eine bestimmte App, Windows Update).
2. **Öffnen Sie O&O ShutUp10** und suchen Sie nach Einstellungen, die mit der betroffenen Funktion zusammenhängen. Die Einstellungen sind nach Kategorien organisiert (Suche, Windows Update, Sicherheit usw.).
3. **Schalten Sie die verdächtigte Einstellung zurück** (von Grün auf Rot), um den Windows-Standard für diese Funktion wiederherzustellen.
4. **Testen** Sie, ob das Problem behoben ist.
5. Wenn Sie die spezifische Einstellung nicht identifizieren können, verwenden Sie **Aktionen → Alle Änderungen rückgängig machen**, um alle Windows-Standards wiederherzustellen, und wenden Sie dann Einstellungen Kategorie für Kategorie erneut an, um die Ursache zu isolieren.
6. Als letzten Ausweg verwenden Sie die **Windows-Systemwiederherstellung**, um zu einem Wiederherstellungspunkt zurückzukehren, der erstellt wurde, bevor Sie die Änderungen angewendet haben.

Einstellungen werden automatisch von Windows zurückgesetzt

Warum werden einige Einstellungen nach dem Anwenden wieder zurückgesetzt?

Bestimmte Datenschutz- und Telemetrieoptionen in Windows werden regelmäßig durch Windows-Komponenten zurückgesetzt, auch ohne Benutzereingriff. Dies liegt an der internen Verwaltung entsprechender Registrierungswerte durch Windows und ist kein Fehler von O&O ShutUp10.

Welche Einstellungen sind besonders betroffen?

Beispiele:

- Bing Websuche in Windows-Suche deaktivieren (z.B. M003)
- Edge-Standardbrowser-Aufforderungen (HKCU) deaktivieren
- Peer-to-Peer für Windows-Updates deaktivieren
- Nutzung von Standortdaten durch Cortana/Suche unterbinden
- Websuche in der Windows-Desktopsuche deaktivieren
- Feedbackanfragen deaktivieren
- Internetzugriff für Windows Media DRM deaktivieren

Warum wird M003 besonders häufig zurückgesetzt?

- Der Windows-Suchdienst kann Werte bei Neustart oder Wiederherstellung zurücksetzen.
- Windows Explorer und Gruppenrichtlinienaktualisierungen können ebenfalls Änderungen aufheben.
- Auch durch Windows-Updates und geplante Aufgaben kann ein Zurücksetzen erfolgen.

Was leistet ShutUp10 Premium?

Die Premium-Version setzt zurückgesetzte Einstellungen automatisch erneut. Wird ein "Ping-Pong-Effekt" erkannt (ständiges Zurücksetzen durch Windows), wird die betreffende Einstellung vorübergehend vom Schutz ausgenommen, um unnötige Aktivitäten

und Benachrichtigungen zu vermeiden. Nutzer erhalten eine Benachrichtigung und können die Überwachung in den Einstellungen wieder aktivieren.

In der Free Edition

Einstellungen müssen manuell erneut gesetzt werden. Häufig zurückgesetzte Optionen werden ohne Nachbearbeitung wieder deaktiviert.

Unternehmen und fortgeschrittene Anwendungsfälle

Kann ich O&O ShutUp10 in einer Unternehmensumgebung verwenden?

Ja. Die **Premium Edition** ist speziell für den Unternehmenseinsatz konzipiert. Sie bietet:

- **Client/Service-Architektur** — Ein Hintergrunddienst wendet Datenschutzeinstellungen an und pflegt sie, ohne Endbenutzer-Interaktion oder Administratorrechte zu erfordern.
- **Automatische Neuanwendung** — Der Dienst erkennt, wenn Windows-Updates oder Gruppenrichtlinienänderungen Einstellungen zurücksetzen, und wendet Ihre bevorzugte Konfiguration erneut an.
- **Zentrale Konfiguration** — Administratoren können ein Standard-Datenschutzprofil definieren und es über mehrere Endpunkte hinweg bereitstellen.

Die **Free Edition** kann ebenfalls in Unternehmensumgebungen verwendet werden, erfordert aber die manuelle Ausführung mit Administratorrechten auf jedem Rechner, was sie für großflächige Bereitstellungen weniger praktisch macht.

Kann ich O&O ShutUp10-Einstellungen über die Befehlszeile oder ein Skript bereitstellen?

Ja. O&O ShutUp10 unterstützt den Befehlszeilenbetrieb, der die Integration mit Bereitstellungsskripten, Anmeldeskripten oder Verwaltungstools ermöglicht. Sie können ein gespeichertes Profil (`.cfg` -Datei) unbeaufsichtigt von der Befehlszeile aus anwenden, was es für die automatisierte Bereitstellung über mehrere Rechner hinweg geeignet macht.

Wie interagiert O&O ShutUp10 mit Gruppenrichtlinieneinstellungen?

O&O ShutUp10 wendet Einstellungen über die Windows-Registry an, was der gleiche Mechanismus ist, der von Gruppenrichtlinien verwendet wird. Im Allgemeinen:

- Wenn eine Einstellung durch **lokale Gruppenrichtlinie** verwaltet wird, kann O&O ShutUp10 sie überschreiben (da beide an die gleichen Registry-Speicherorte schreiben).
- Wenn eine Einstellung durch **Domänen-Gruppenrichtlinie** (in einer Active Directory-Umgebung) durchgesetzt wird, hat die Domänenrichtlinie Vorrang und kann von O&O ShutUp10 vorgenommene Änderungen überschreiben.

> **Info**
>
> In Unternehmensumgebungen wird empfohlen, O&O ShutUp10-Konfigurationen mit Ihrer Gruppenrichtlinienstrategie abzustimmen, um Konflikte zu vermeiden.

Ist O&O ShutUp10 konform mit der DSGVO und anderen Datenschutzvorschriften?

O&O ShutUp10 selbst sammelt, speichert oder überträgt keine Benutzerdaten. Es ist ein lokales Tool, das Windows-Einstellungen auf dem Gerät ändert, auf dem es ausgeführt wird.

Durch die Verwendung von O&O ShutUp10 zum Deaktivieren von Telemetrie-, Tracking- und Datenfreigabefunktionen in Windows können Organisationen das Volumen der an Microsoft übertragenen personenbezogenen Daten reduzieren — was die Compliance mit der **Datenschutz-Grundverordnung (DSGVO)**, dem **CCPA** und anderen Datenschutzrahmenwerken unterstützen kann. O&O ShutUp10 ist jedoch eine Komponente einer umfassenderen Compliance-Strategie; Organisationen sollten ihre Datenschutzbeauftragten und Rechtsteams für umfassende Compliance-Beratung konsultieren.

Wo bekomme ich Hilfe, wenn meine Frage hier nicht beantwortet wird?

- **O&O Software Support:** https://www.oo-software.com/en/support
- **O&O Software Produktseite:** https://www.oo-software.com/en/shutup10
- **Microsoft Datenschutz-Dokumentation:** https://privacy.microsoft.com
- **Microsoft Windows Datenschutzeinstellungen Referenz:** https://support.microsoft.com/en-us/windows/windows-privacy-settings

Für Premium Edition-Kunden ist prioritärer Support über das O&O Software-Support-Portal verfügbar.