O&O software

O&O ShutUp10++

Table of Contents

O&O ShutUp10 Documentation

Welcome to the official documentation for **O&O ShutUp10** — the free and premium antispy tool for Windows 10 and Windows 11 by O&O Software GmbH.

What is O&O ShutUp10?

O&O ShutUp10 gives you full control over the privacy settings in Windows 10 and Windows 11. It allows you to decide which unwanted functions should be deactivated, keeping your personal data private. The tool manages a wide range of Windows privacy and telemetry settings in a single, easy-to-use interface — no deep registry knowledge required.

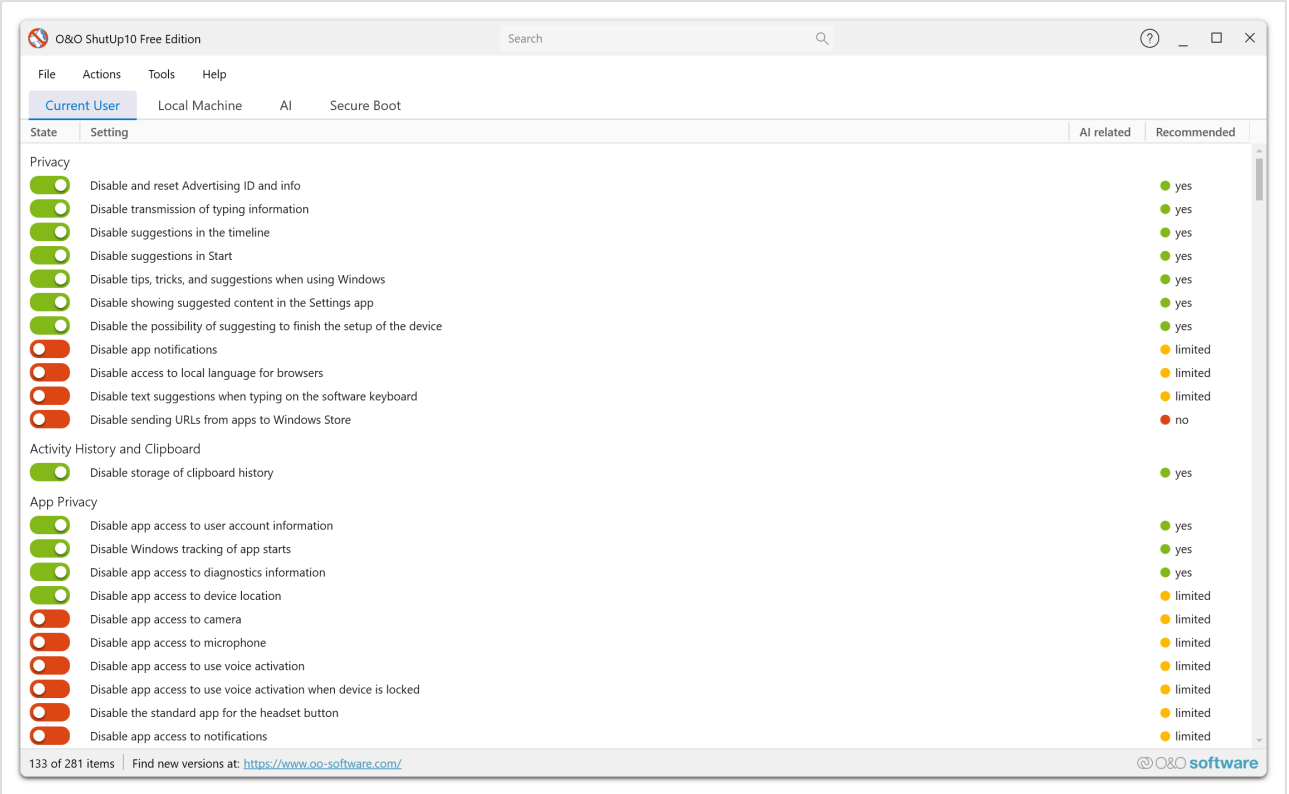
Key Benefits

- **Full privacy control** — Manage almost 300 privacy-related settings in Windows 10 and Windows 11.
- **No installation required (Free Edition)** — Run it directly as a portable application.
- **Clear recommendations** — Each setting includes a recommendation level so you know what is safe to change.
- **Undo changes at any time** — All modifications can be reverted with a single click.
- **Completely free (Free Edition)** — The Free Edition is and will remain free of charge.

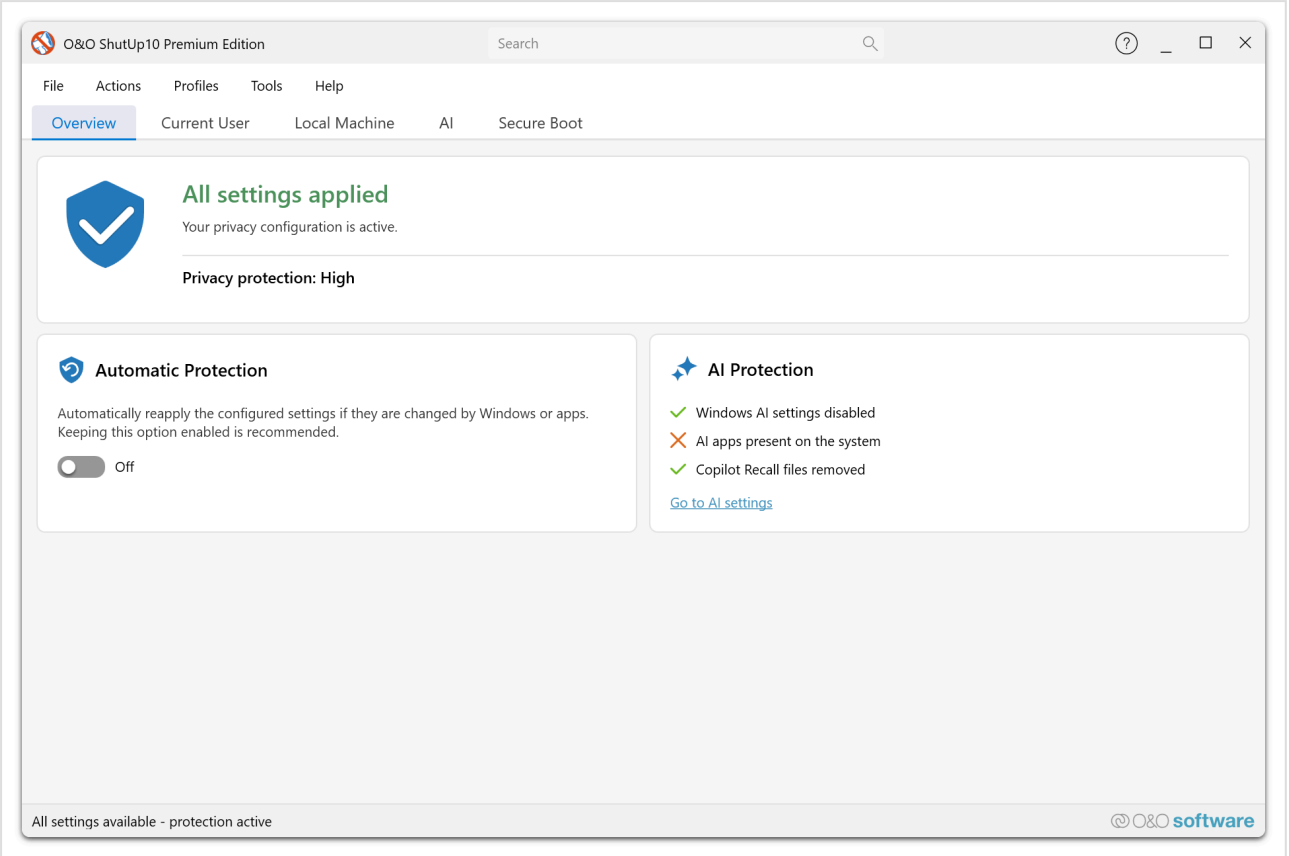
Editions Overview

O&O ShutUp10 is available in two editions, each designed for different use cases and environments.

Free Edition



Premium Edition



Free Edition

The **Free Edition** is a portable, standalone tool that requires no installation. It is a powerful choice for individual users who want full, immediate control over their Windows privacy settings — covering nearly 300 settings with clear recommendations and zero cost.

- Portable — runs directly from the executable, no setup needed.
- Full privacy settings coverage — the same ~300 settings as the Premium Edition.
- Each privacy change is applied interactively by the user.
- **Requires administrator rights** for every execution, since it modifies system-level settings.
- Perfect for home users, privacy audits, and individual workstations.

➡️ Learn more about the Free Edition

Premium Edition — *Stay private. Forever.*

The **Premium Edition** is designed for professional and enterprise environments. It uses a client/service architecture that provides automatic and proactive privacy protection — ensuring your settings stay enforced even after Windows updates.

- Uses a **client/service model** — the service runs in the background and applies settings automatically.
- **Proactive protection** — automatically re-applies your preferred settings after Windows updates or policy changes.
- **Does not require end-user administrator rights** — the background service handles all privileged operations.
- Ideal for corporate environments, managed workstations, and IT departments.

➡️ Learn more about the Premium Edition

How to Use This Documentation

Use the sidebar navigation to explore features and find detailed information:

- **Free Edition** and **Premium Edition** sections describe the specific capabilities and workflows of each edition.
- The **Features** section covers all privacy and configuration settings. Features exclusive to the Premium Edition are marked with a Premium badge.

Feature Comparison

O&O ShutUp10 is available in two editions. The **Free Edition** is a portable, interactive privacy tool for individual users. The **Premium Edition** adds a client/service architecture with automatic enforcement, making it suitable for professional and enterprise environments.

This page provides a detailed comparison of both editions and explains why O&O ShutUp10 offers more reliable privacy enforcement than Group Policy Objects (GPO).

Edition Comparison Table

Feature	Free Edition	Premium Edition
Privacy settings management (~300 settings)	✅	✅
Recommendation levels for each setting	✅	✅
Create and restore system points	✅	✅
Apply/undo recommended settings in bulk	✅	✅
Profiles and export/import	✅	✅
AI Removal (Copilot & Recall)	✅	✅
Edit Mode for advanced users	✅	✅
Portable — no installation required	✅	—
Client/service architecture	—	✅
Automatic re-application after Windows Updates	—	✅
Automatic re-application after Group Policy changes	—	✅
Continuous background monitoring	—	✅
No end-user administrator rights required	—	✅
Profiles Editor for centralized policy management	—	✅
Suitable for corporate/enterprise deployment	—	✅

What the Premium Edition Adds

Automatic Protection

The most significant advantage of the Premium Edition is **Automatic Protection**. The Free Edition applies settings only when a user runs the application manually — if a Windows update or policy change resets those settings, the user must re-check and re-apply them by hand.

The Premium Edition runs a background service that **continuously monitors** privacy-related registry values. When it detects that a setting has been changed — whether by a Windows update, a Group Policy push, or any other system modification — it **automatically re-applies** the preferred configuration without user intervention.

➡️ Learn more about Automatic Protection

Client/Service Architecture

The Premium Edition separates the user interface (client) from the enforcement engine (service):

- **The Service** runs as a Windows service with system-level privileges, handling all privileged operations in the background.
- **The Client** is a standard user application that communicates with the service — no administrator rights needed.

This architecture is essential in corporate environments where end users do not have admin rights. The Free Edition, by contrast, requires administrator privileges for every execution.

Profiles Editor

The Premium Edition includes a **Profiles Editor** that allows IT administrators to create, edit, and deploy standardized privacy configurations across multiple workstations. This enables centralized policy management without requiring each user to configure settings individually.

➡️ Learn more about the Profiles Editor

Why O&O ShutUp10 Is Superior to GPO for Privacy Enforcement

Many IT administrators rely on Group Policy Objects (GPO) to manage Windows privacy settings. While GPO is a powerful tool for system configuration, it has well-documented limitations when it comes to **persistent enforcement of privacy settings** — particularly across Windows updates.

The Problem: Windows Updates Can Reset GPO-Managed Privacy Settings

Microsoft's cumulative and feature updates are known to reset or override privacy-related settings, even when those settings were previously configured through Group Policy. This behavior has been documented in several contexts:

- **Feature updates reset local and registry-based privacy settings.** Major Windows feature updates (e.g., semi-annual channel releases) can reset privacy-related registry values and local Group Policy settings to their defaults. Microsoft's own documentation acknowledges that feature updates effectively perform an in-place upgrade, which can overwrite prior configurations. (Microsoft Learn — Windows feature update overview)
- **Group Policy re-application depends on the policy refresh cycle.** Even when domain-based GPOs are used, settings are only re-applied during the Group Policy refresh interval (typically every 90 minutes ± 30 minutes for computer settings). Between a Windows update resetting a value and the next GPO refresh, the system runs with default (less private) settings. (Microsoft Learn — Group Policy processing))
- **Not all privacy settings are exposed through Group Policy.** Some Windows privacy and telemetry settings can only be configured via direct registry modification and have no corresponding Group Policy administrative template. GPO cannot

enforce settings that are not represented in its ADMX/ADML templates. (Microsoft Learn — Manage connections from Windows to Microsoft services)

- **Local Group Policy (non-domain) is particularly vulnerable.** Machines not joined to an Active Directory domain rely on local Group Policy, which is even more susceptible to being overwritten during feature updates. Local policy settings stored in the registry under `HKLM\SOFTWARE\Policies` can be cleared or reset by the update process.

How O&O ShutUp10 Premium Solves This

O&O ShutUp10 Premium's Automatic Protection addresses each of these limitations:

Limitation of GPO	O&O ShutUp10 Premium
Settings can be reset by Windows feature updates	The background service detects changes and re-applies settings **immediately** — no waiting for a policy refresh cycle.
GPO refresh only occurs every ~90 minutes	The service monitors registry values **continuously** and responds to changes as they happen.
Some privacy settings have no GPO equivalent	O&O ShutUp10 manages settings through direct registry modification, covering settings that have **no ADMX/ADML template**.
Local Group Policy is overwritten by feature updates	The service stores the desired configuration independently of Group Policy, so it can re-apply settings **regardless of what the update process changes**.
Requires Active Directory infrastructure for domain GPO	O&O ShutUp10 works on **standalone machines** and domain-joined machines alike — no AD infrastructure required.

When GPO Is Still Appropriate

Group Policy remains the right tool for many system configuration tasks — software deployment, security baselines, drive mappings, and logon scripts, among others. The point above is specifically about **privacy and telemetry settings**, where the combination of frequent Windows updates and incomplete ADMX coverage makes GPO enforcement unreliable without a supplementary tool.

O&O ShutUp10 Premium can work **alongside** Group Policy as a complementary enforcement layer, ensuring that privacy settings remain consistent even when GPO alone cannot guarantee it.

References

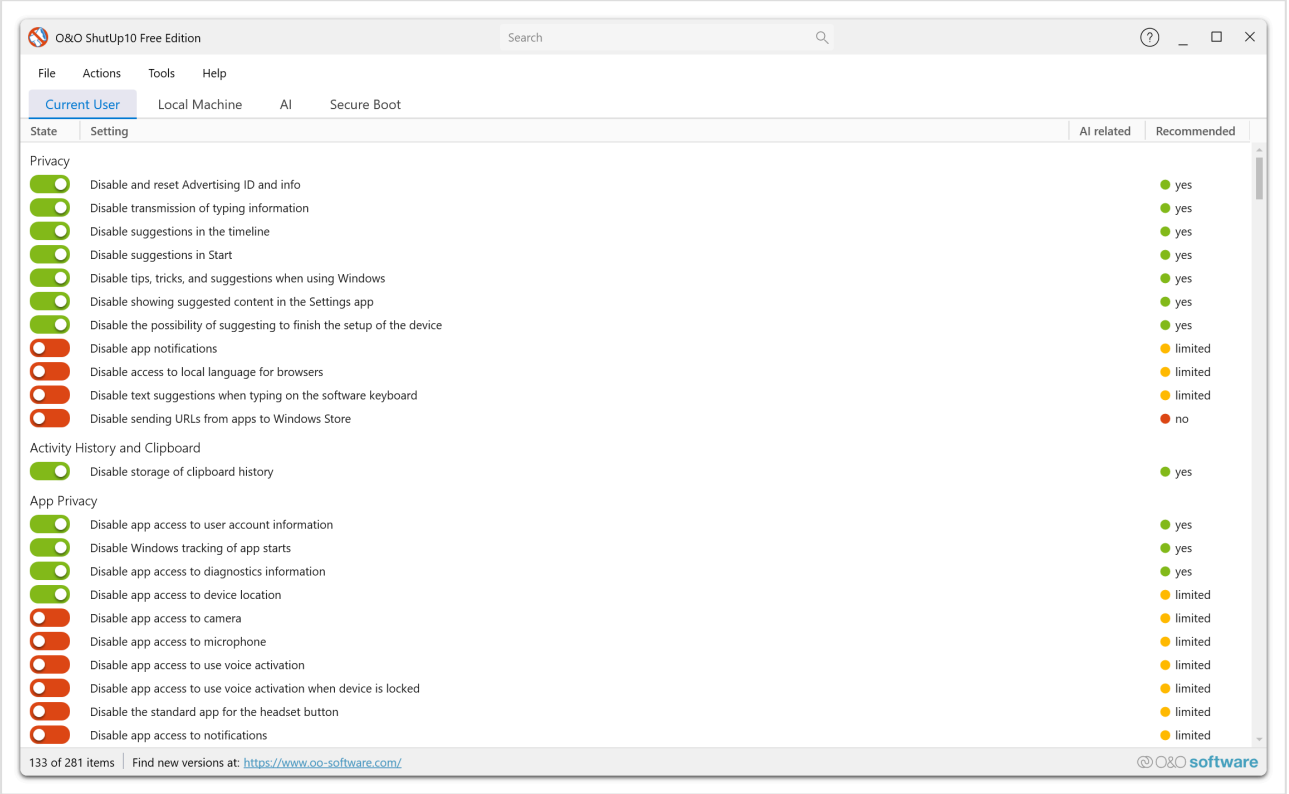
1. Microsoft Learn — *How Windows Update works*: https://learn.microsoft.com/en-us/windows/deployment/update/how-windows-update-works
2. Microsoft Learn — *Group Policy processing and precedence*: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11))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

Summary

	GPO Only	O&O ShutUp10 Free	O&O ShutUp10 Premium
Covers all Windows privacy settings	Partial	✅	✅
Survives Windows feature updates automatically	❌	❌ (manual re-check)	✅
Continuous monitoring and re-application	❌	❌	✅
Works without Active Directory	Local GPO only	✅	✅
No admin rights needed for end users	Depends on setup	❌	✅
Centralized profile management	Via AD/GPO	Export/Import	✅ Profiles Editor

O&O ShutUp10 Free Edition

The **Free Edition** of O&O ShutUp10 is a powerful, portable privacy tool for Windows 10 and Windows 11. It gives you full, immediate control over your Windows privacy settings — without requiring installation, subscriptions, or technical expertise. Simply download, run, and take charge of your data.



How It Works

O&O ShutUp10 Free Edition runs as a standalone portable executable. When launched, it scans your current Windows privacy and telemetry settings and presents them in an organized list with clear toggle switches.

1. **Download** the executable from the O&O Software website.
2. **Run** it directly — no installation needed.
3. **Review** the list of privacy settings, each with a recommendation level.
4. **Toggle** settings on or off to match your privacy preferences.
5. **Apply** your changes and close the application.

> **Info**
>
> **Administrator Rights Required:** The Free Edition always requires administrator privileges because it directly modifies Windows system settings and registry values. You will be prompted by Windows User Account Control (UAC) each time you run it.

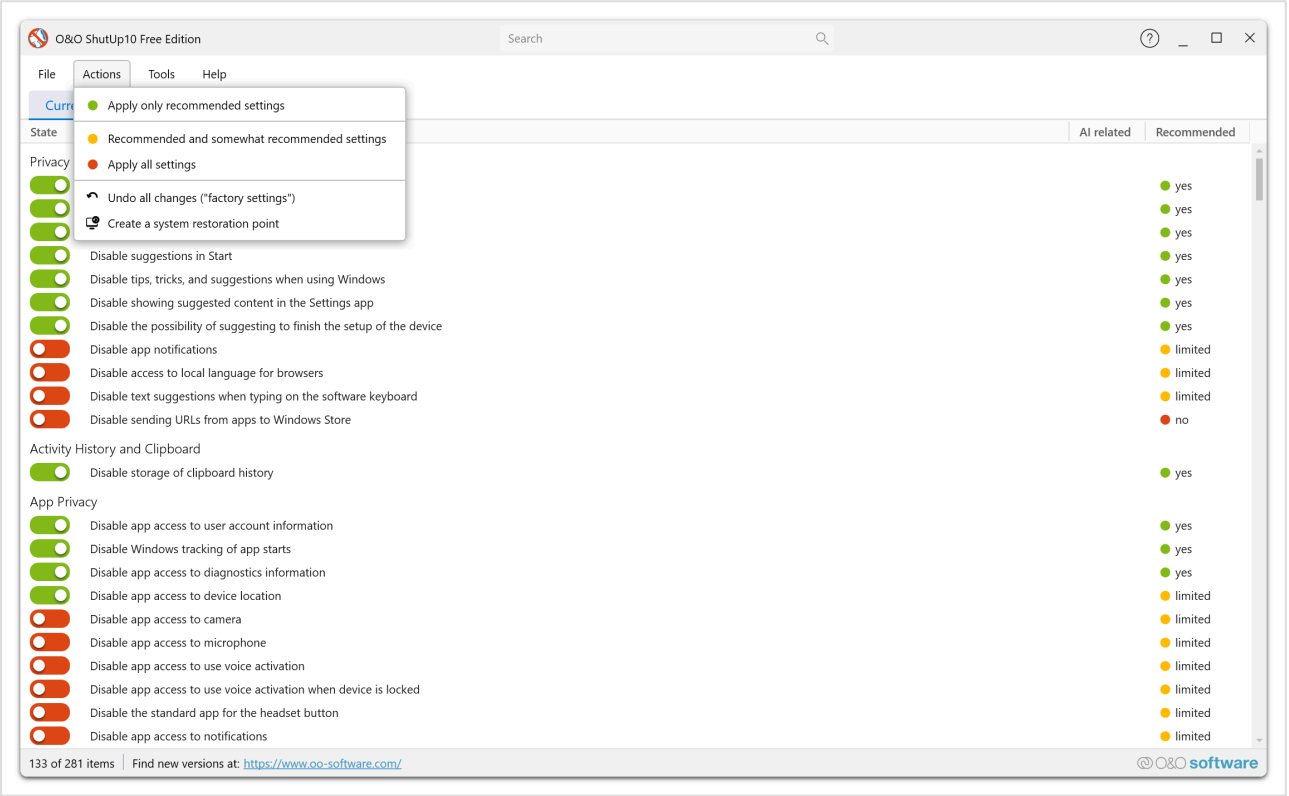
Key Features

Portable Application

No installation, no background services, no leftover files. Simply download, run, and manage your privacy settings. Ideal for USB drives and one-time privacy audits.

Interactive Privacy Management

Every change is made interactively by the user. You review each setting, see its current state, and decide whether to enable or disable it. Nothing changes without your explicit action.



Recommendation Levels

Each setting is assigned a recommendation level to help you decide what to change:

- **Recommended** — Safe to apply for most users; no negative impact on functionality.
- **Limited recommended** — Generally safe, but may affect certain features.
- **Not recommended** — May impact important Windows functionality; apply only if you understand the consequences.

Create and Restore System Points

Before making changes, you can create a system restore point. If something does not work as expected, you can easily undo all changes.

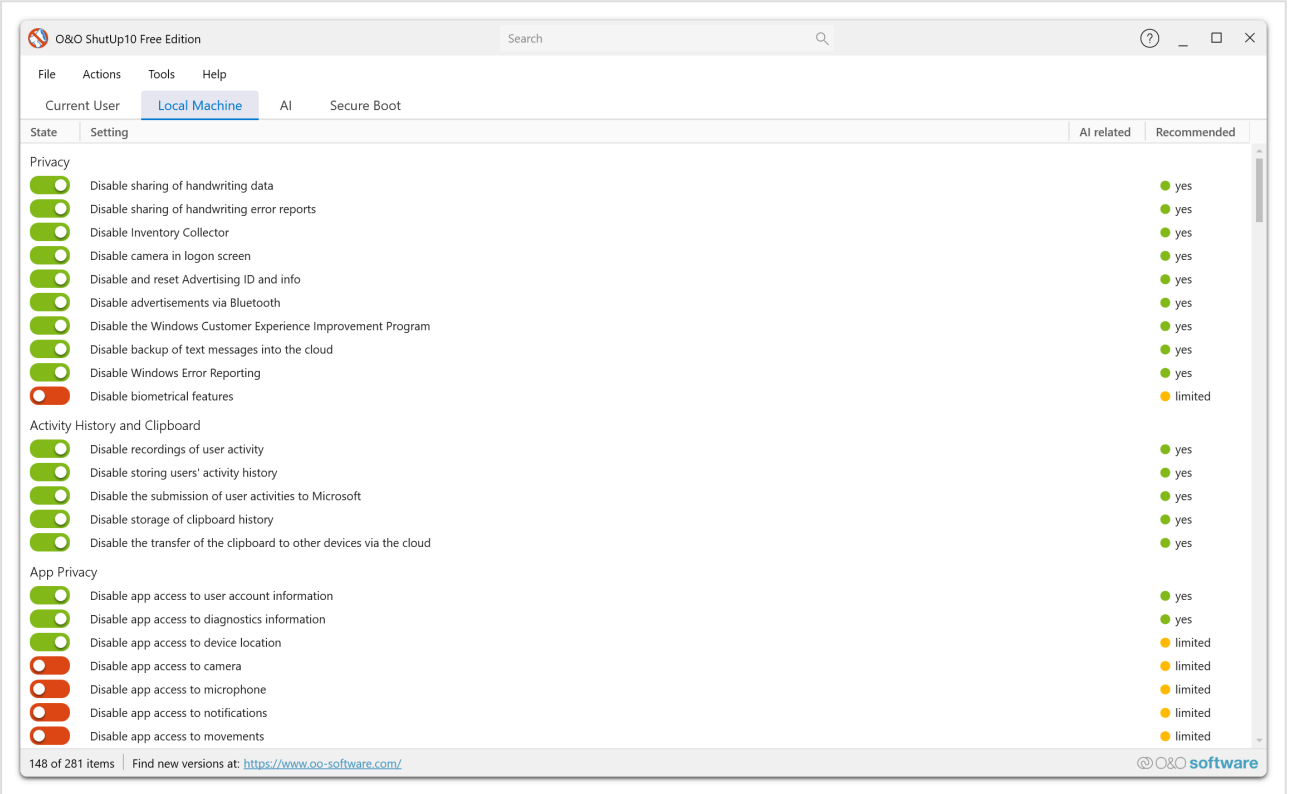
Apply Recommended Settings

Apply all recommended settings at once instead of toggling each one individually. You can also undo all changes or reset everything to Windows defaults.

Current User and Local Machine Tabs

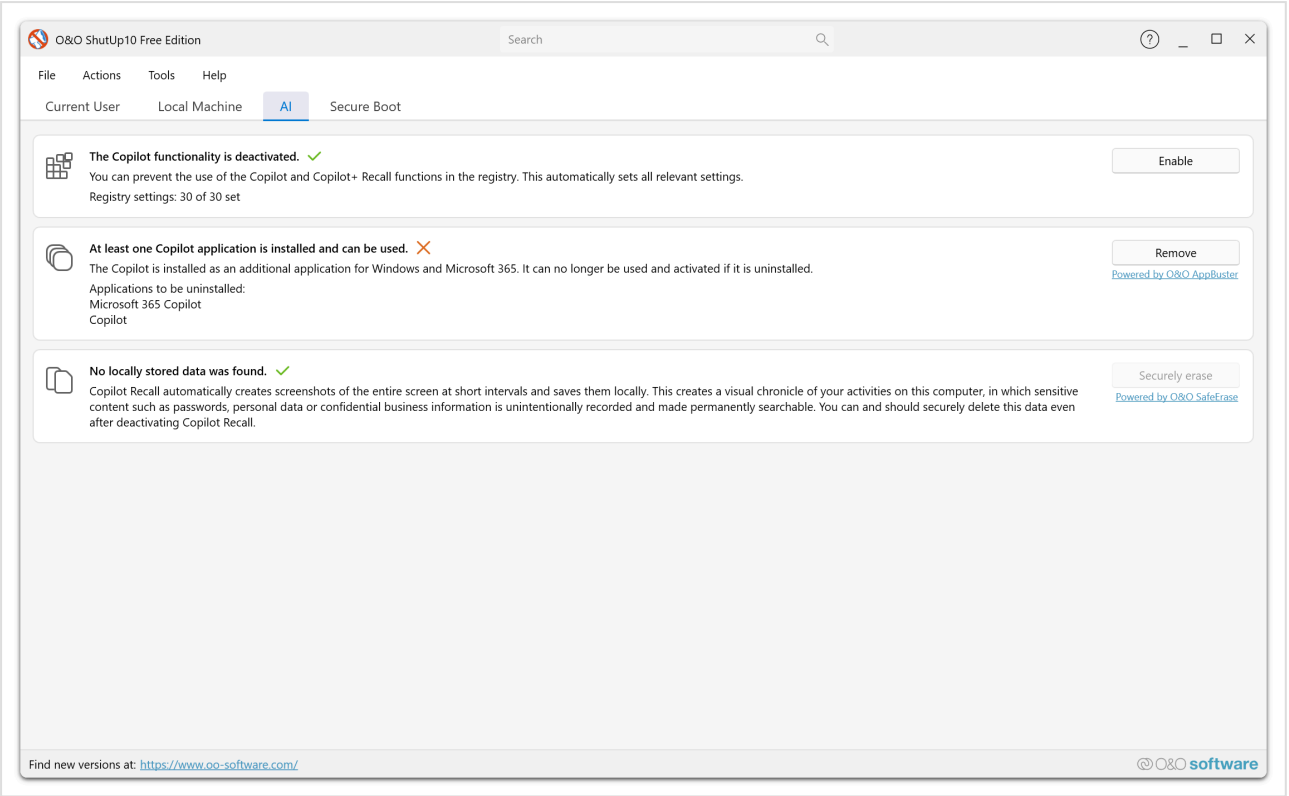
The Free Edition organizes privacy settings into two main scope tabs:

- **Current User** — Settings that apply to the currently logged-in Windows user account (e.g., privacy preferences, app permissions, advertising ID).
- **Local Machine** — Settings that apply system-wide to all users on the computer (e.g., telemetry, error reporting, Bluetooth advertising).



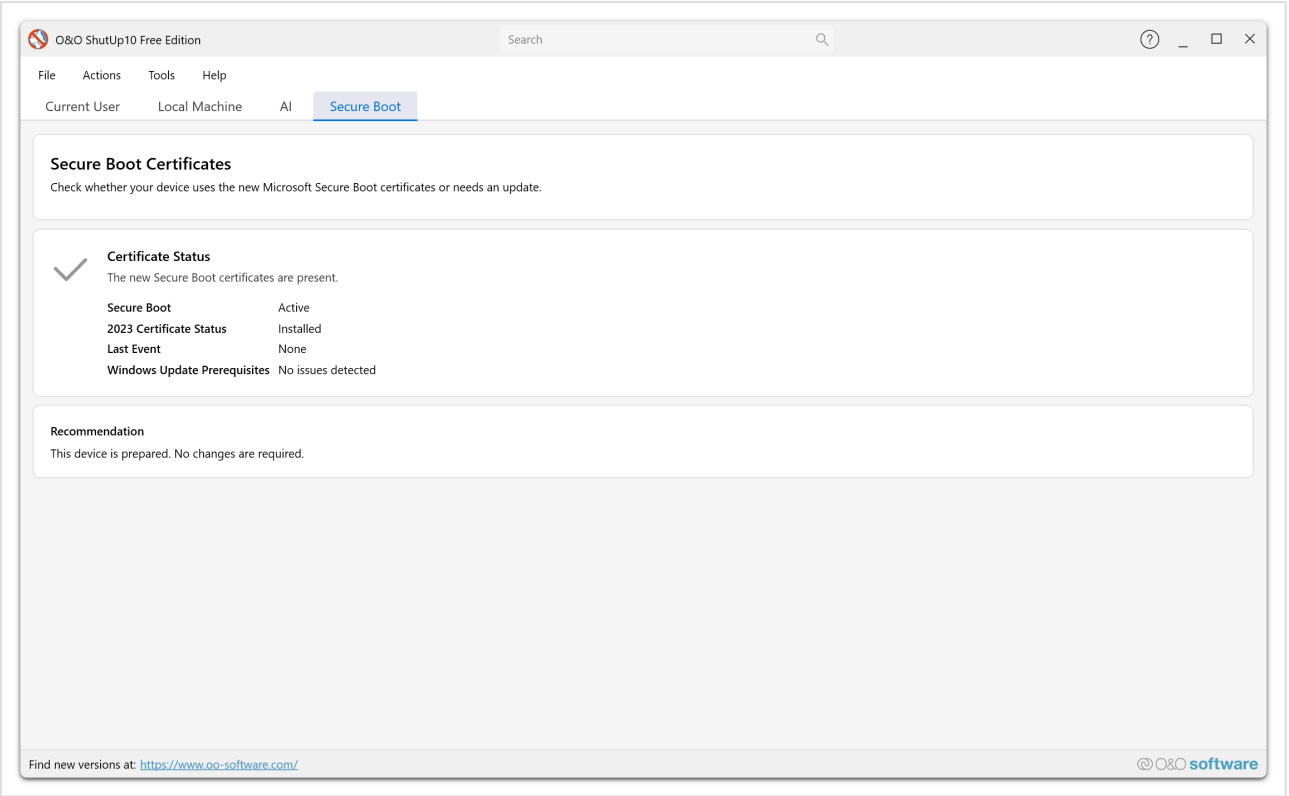
AI Removal

The Free Edition includes the full AI Removal feature for disabling Microsoft Copilot and Recall components. The **AI** tab provides a three-layer approach: disabling AI-related registry settings, removing Copilot applications, and securely erasing Recall data.



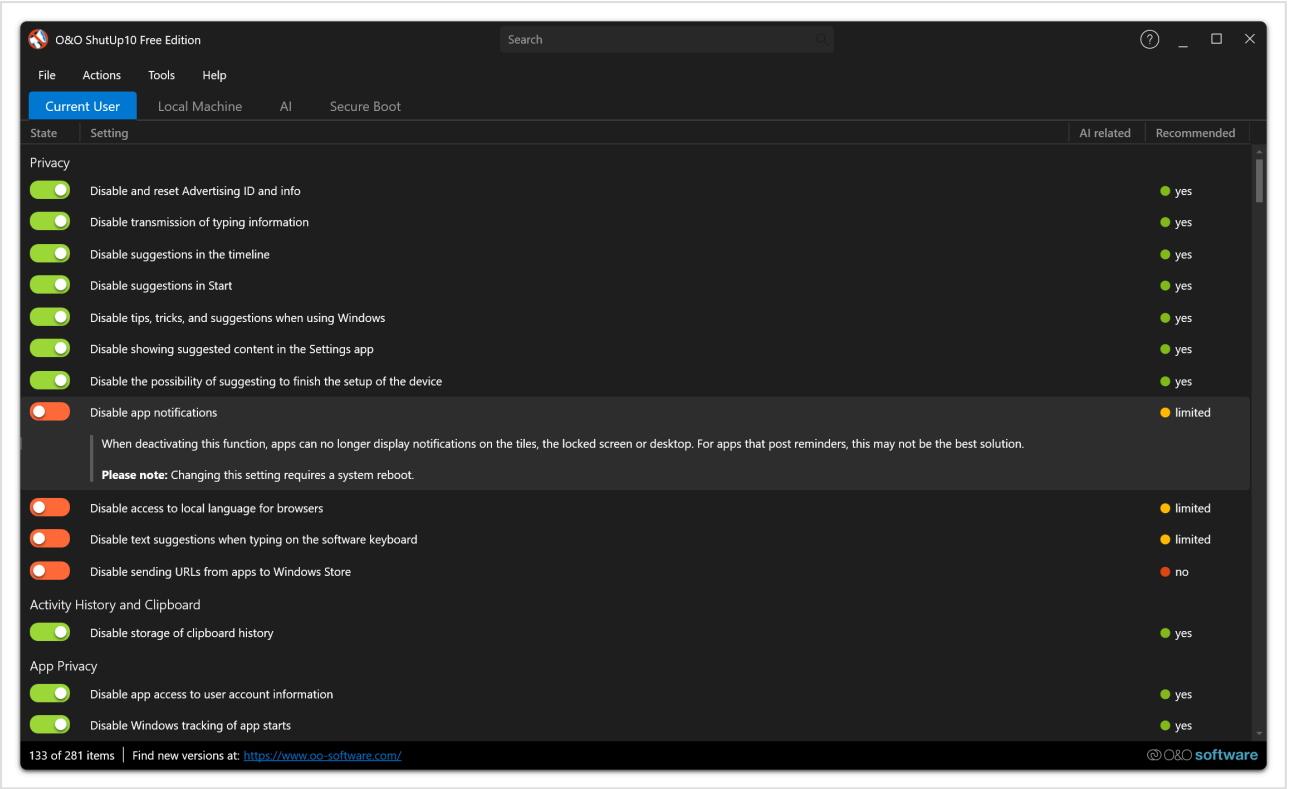
Secure Boot Certificates

The **Secure Boot** tab checks whether your device uses the latest Microsoft Secure Boot certificates or needs an update. It displays certificate status, last event information, and a recommendation for any required action.



Dark Mode Support

The Free Edition supports light and dark mode themes. The display mode follows your Windows system setting by default, or you can select a specific mode in the Settings dialog.



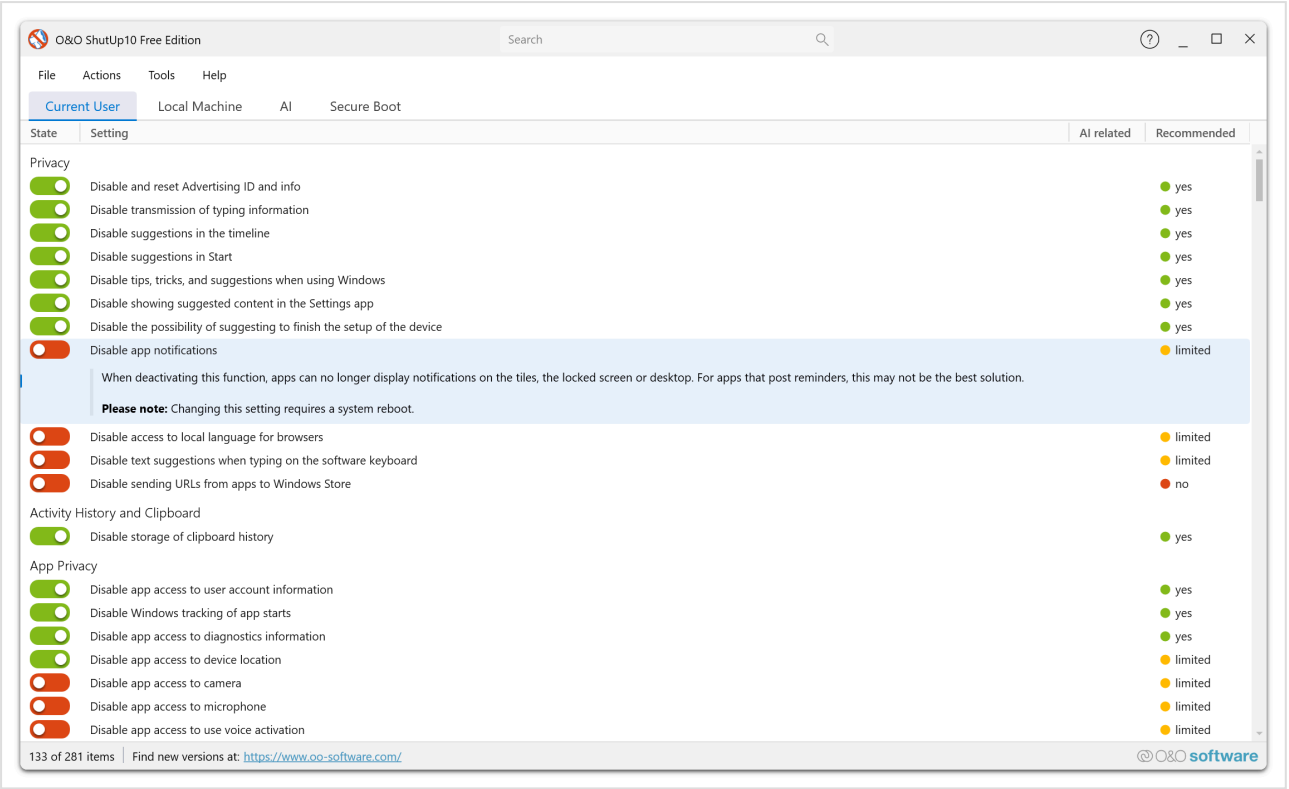
Settings Categories

The Free Edition covers all core privacy setting categories:

- Privacy settings
- Telemetry and data collection
- Location services
- Cortana and search
- Windows Update behavior
- App permissions and access
- Windows Explorer and advertising
- Security-related settings

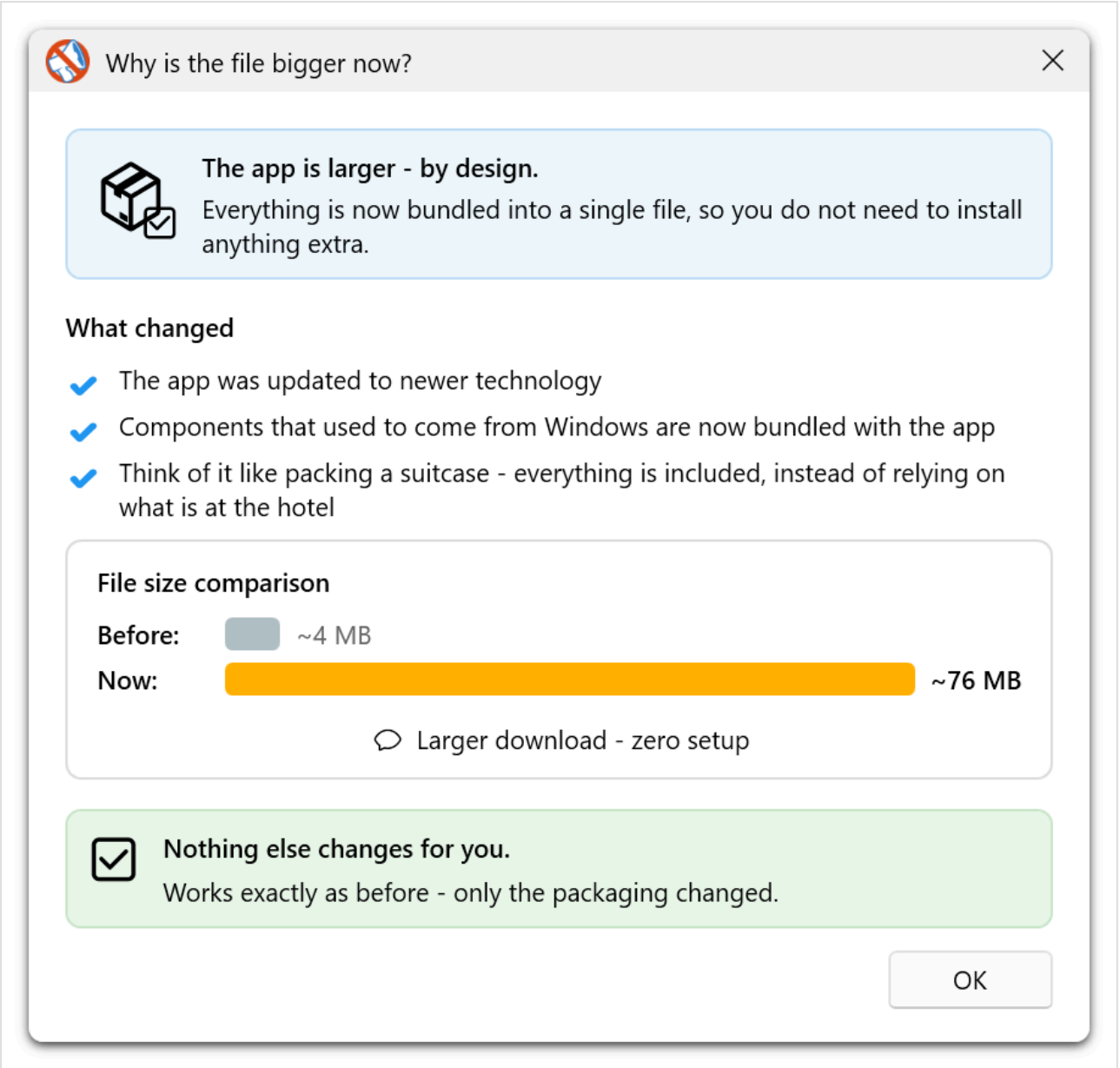
Setting Details

Click on any setting to expand its description. The expanded view shows a detailed explanation of what the setting does, its potential impact, and any notes such as whether a system reboot is required after changing it.



File Size Information

When you first download the Free Edition, you may notice it is larger than older versions. The application displays an informational dialog explaining this change:



The increased file size is by design: all runtime components that previously came from Windows are now bundled directly into the executable. This ensures the application works reliably on any system without depending on pre-installed frameworks. The functionality remains identical — only the packaging has changed.

Who Is the Free Edition For?

The Free Edition is the ideal choice for anyone who wants immediate, no-compromise privacy control:

- **Home users** who want a quick, effective way to control their Windows privacy settings.
- **Technical users** who perform privacy audits on individual machines.
- **IT professionals** who need a portable tool for spot-checking privacy configurations.
- **Privacy-conscious users** who want a trusted, proven solution without cost barriers.

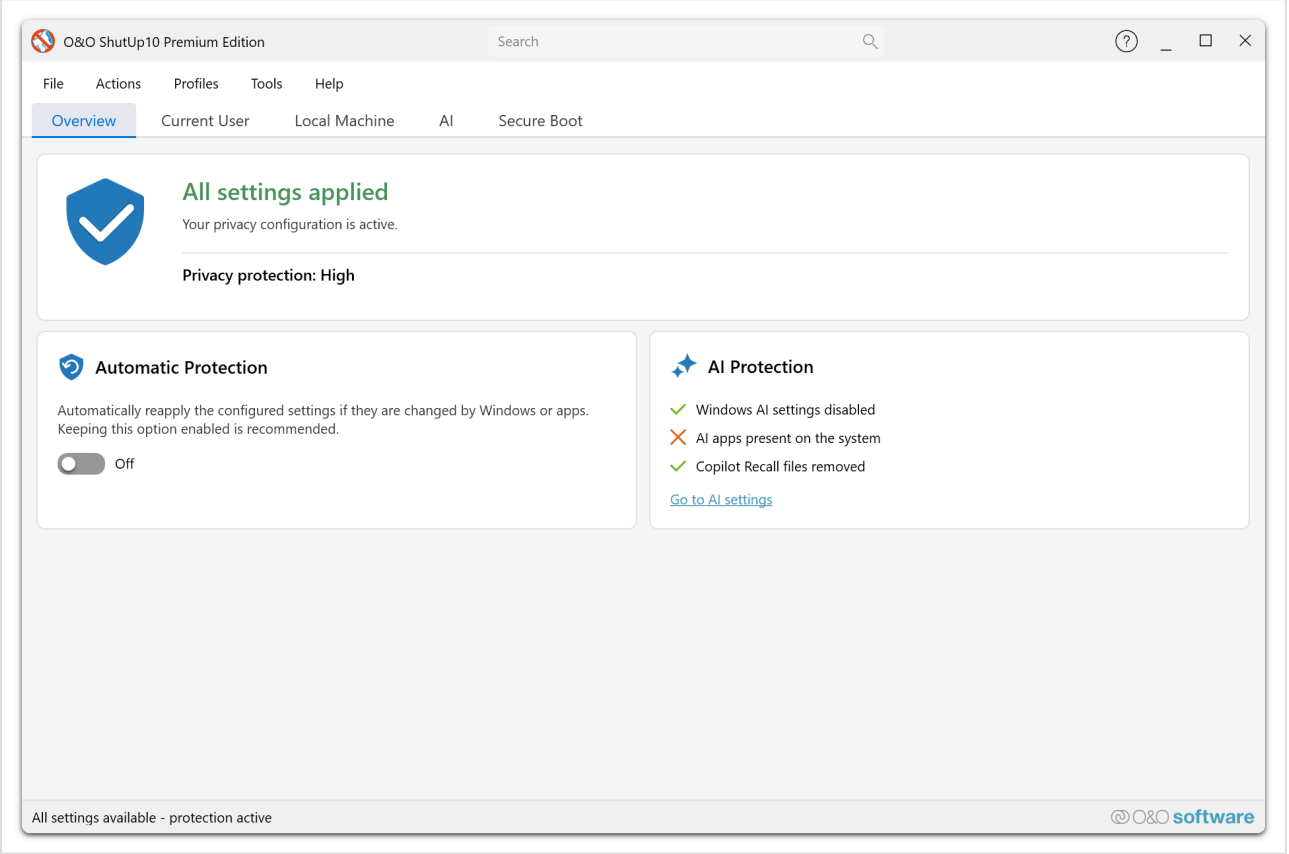
The Free Edition provides the same comprehensive privacy settings coverage as the Premium Edition — nearly 300 settings — making it a complete privacy solution for individual use.

For environments that require automatic protection or operation without end-user administrator rights, see the Premium Edition.

O&O ShutUp10 Premium Edition

> **Stay private. Forever.**

The **Premium Edition** of O&O ShutUp10 is designed for professional and enterprise environments. It uses a client/service architecture that provides automatic, continuous privacy protection — without requiring end-user administrator rights.

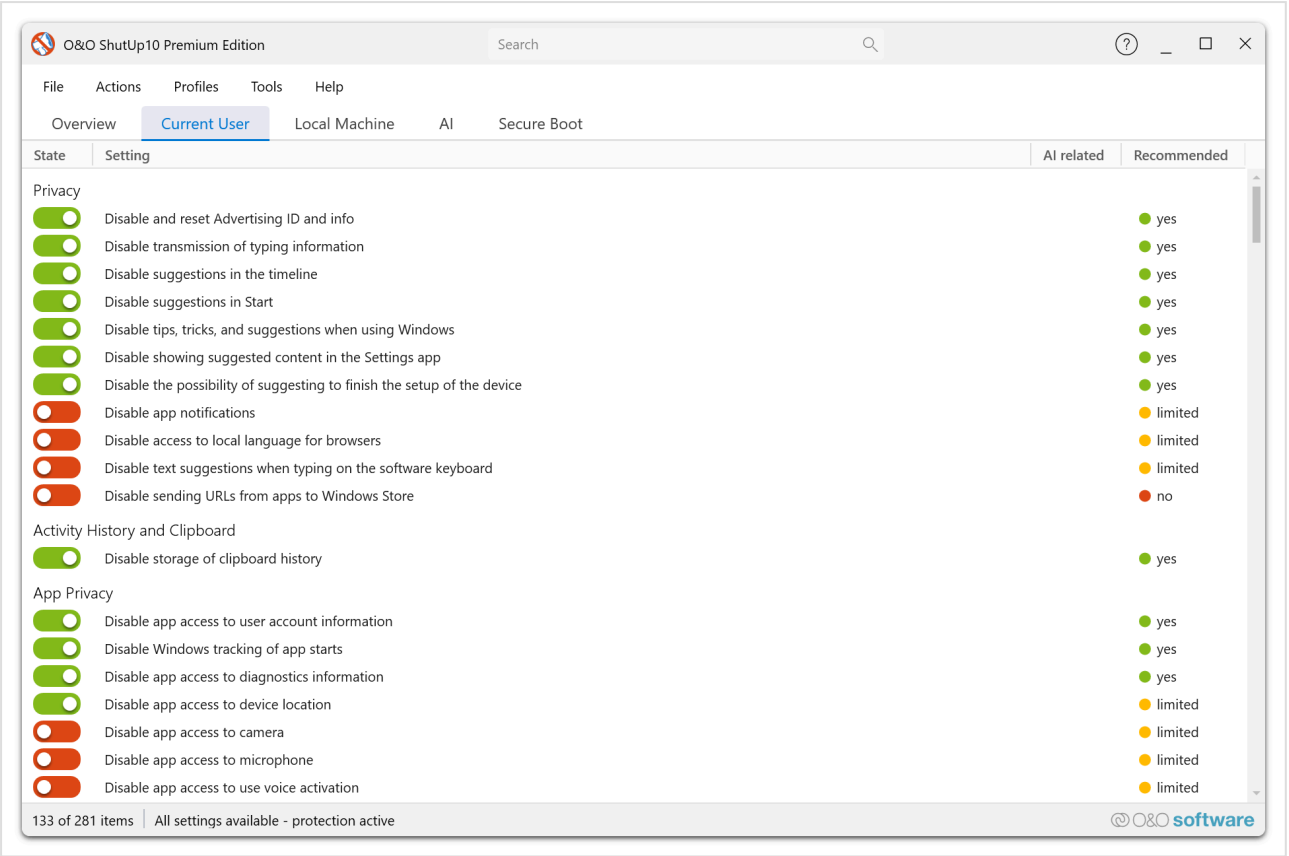


How It Works

The Premium Edition consists of two components:

1. **The Service** — A Windows service running in the background with the necessary system privileges. It monitors and applies your privacy settings automatically.
2. **The Client** — A user-facing application that communicates with the service. Users can view and configure settings without needing administrator rights.

This separation means that the service handles all privileged operations, while end users interact with the client application using their standard Windows account.



Key Features

Client/Service Architecture

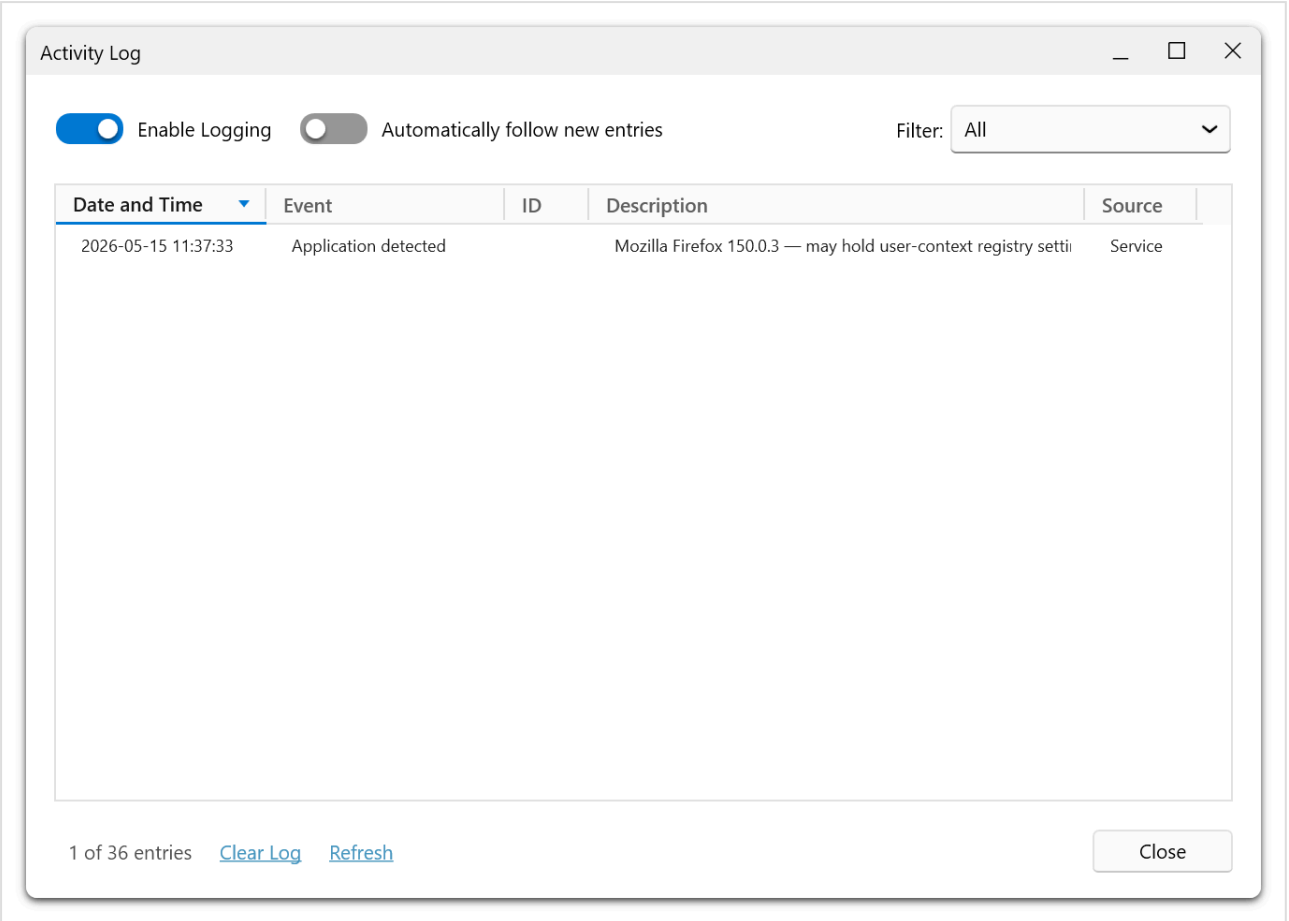
Unlike the Free Edition, which requires admin rights for every execution, the Premium Edition runs a background service that holds the necessary privileges. End users interact through the client without needing elevated permissions.

Proactive Protection

The service continuously monitors your privacy settings and automatically re-applies your preferred configuration after:

- **Windows updates** that may reset privacy settings.
- **Group Policy changes** that override local preferences.
- **System configuration changes** that affect privacy-related registry values.

This ensures your privacy settings remain consistent over time without manual intervention.



No End-User Administrator Rights Required

In corporate environments, most users do not have admin rights. The Premium Edition solves this by delegating all privileged operations to the background service. Users can view and manage their privacy preferences through the client without UAC prompts or admin credentials.

Automatic Protection Premium

Set your preferred privacy configuration once, and the service keeps it enforced automatically. No need for users to re-run the application or manually check settings.

All Free Edition Features Included

The Premium Edition includes every feature of the Free Edition, plus the additional capabilities described above:

- All privacy setting categories (telemetry, location, Cortana, Windows Update, app permissions, etc.)
- Recommendation levels for each setting
- System restore point creation
- Apply/undo recommended settings in bulk

Who Is the Premium Edition For?

The Premium Edition is ideal for:

- **Corporate environments** where users should not need administrator rights.
- **IT departments** that require consistent privacy policies across fleets of workstations.
- **Organizations** that need automatic re-application of privacy settings after Windows updates.
- **Managed service providers (MSPs)** who maintain privacy configurations for multiple clients.

For individual use or quick one-time privacy audits, the Free Edition may be sufficient.

First Steps

This guide walks you through the initial setup process after installing O&O ShutUp10. Follow these steps to get started with either the Free Edition or the Premium Edition.

Free Edition — Getting Started

The Free Edition requires no installation. Follow these steps to begin managing your Windows privacy settings:

1. Download and Launch

1. Download the O&O ShutUp10 executable from the O&O Software website.
2. Run the executable directly — no installation is needed.
3. Windows will display a **User Account Control (UAC)** prompt. Click **Yes** to grant administrator rights.

> **Info**
>
> The Free Edition always requires administrator privileges because it directly modifies Windows system settings and registry values.

2. Review Your Privacy Settings

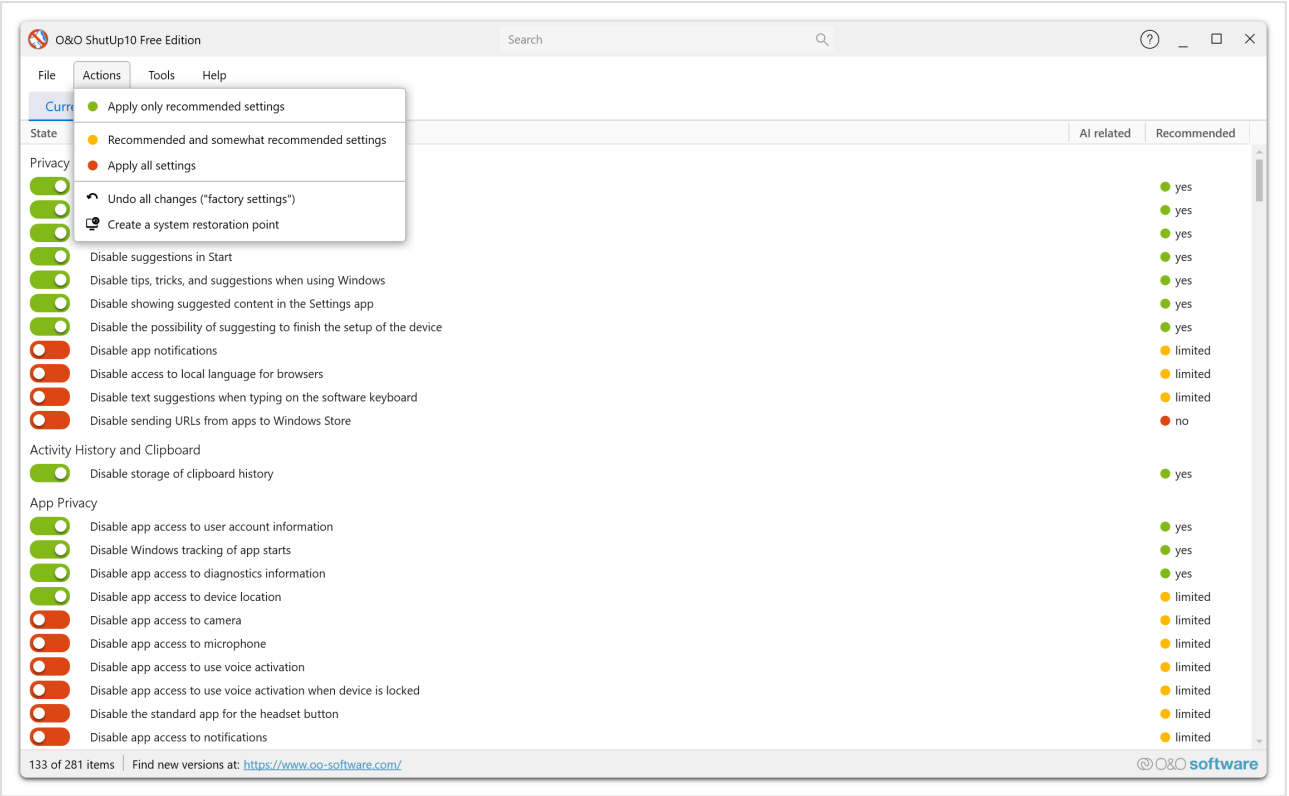
After launching, O&O ShutUp10 scans your current Windows privacy and telemetry settings. The main window displays a categorized list of all available settings, each with:

- A **toggle switch** showing the current state (enabled or disabled).
- A **recommendation level** — Recommended, Limited, or Not Recommended.

Take a moment to review the settings and their recommendation levels before making changes.

3. Create a System Restore Point

Before making any changes, create a system restore point from the **Actions** menu:



1. Open **Actions** → **Create System Restore Point**.
2. Confirm the creation when prompted.

This allows you to revert all changes if something does not work as expected.

4. Apply Recommended Settings

For a quick start, apply all recommended settings at once:

1. Open **Actions** → **Apply All Recommended Settings**.
2. Confirm the action when prompted.

This enables all settings marked as **Recommended** — safe for most users with minimal impact on Windows functionality.

5. Fine-Tune Individual Settings

After applying recommended settings, review the remaining settings and adjust them based on your preferences:

- **Limited recommended** settings are generally safe but may affect certain features.
- **Not recommended** settings may impact important Windows functionality — apply only if you understand the consequences.

6. Close the Application

Once you are satisfied with your settings, simply close the application. Your changes are saved in the Windows registry and persist until changed by you, a Windows update, or another system modification.

> **Tip**
>
> Run O&O ShutUp10 again after each major Windows update to verify that your privacy settings have not been reset.

Premium Edition — Getting Started

The Premium Edition uses a client/service architecture. The initial setup is guided by the **Premium Overview** page, which walks you through each step.

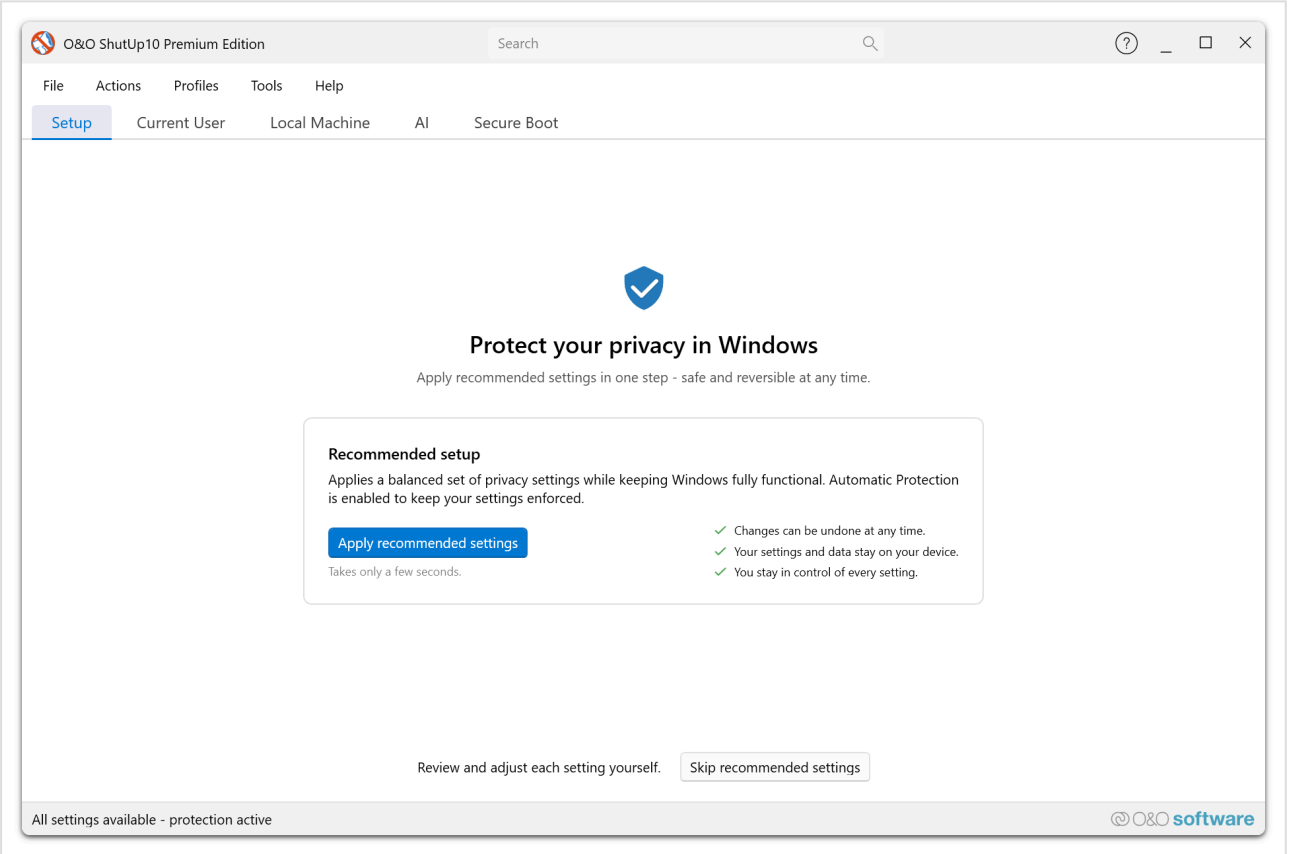
1. Install the Premium Edition

Install O&O ShutUp10 Premium Edition using the provided installer. The installer registers:

- **The Service** — A Windows background service that runs with system privileges.
- **The Client** — The user-facing application for viewing and configuring settings.

2. Launch the Client

After installation, launch the O&O ShutUp10 client application. The **Premium Overview** opens automatically in **Setup Mode**.



3. Complete the Guided Setup

The Premium Overview guides you through the following steps in Setup Mode:

Step	What Happens
Service Installation	The setup verifies that the background service is installed and registered.
Service Connection	The client confirms communication with the background service.
Profile Selection	You are prompted to choose an initial privacy profile (e.g., Recommended Settings).
First Application	The selected profile is applied to establish your baseline privacy configuration.

No administrator rights are required from the end user — the background service handles all privileged operations.

4. Verify Protection Status

Once setup is complete, the Premium Overview transitions to **Overview Mode**, displaying:

- **Protection Status** — Confirms that automatic protection is active.
- **Service Status** — Shows the background service is running.
- **Active Profile** — Displays the name of the applied privacy profile.

5. Configure Additional Settings (Optional)

After the initial setup, you can customize the application further through the **Settings Dialog** (**View** → **Settings…**):

- **Notifications** — Configure how you are notified about automatic protection events.
- **Autostart** — Set the application to start automatically when you log on.
- **Hybrid Mode** — Enable automatic exclusion of settings managed by Group Policy (useful in corporate environments).

For details, see the Settings Dialog documentation.

6. Ongoing Usage

With the Premium Edition, your privacy settings are automatically maintained:

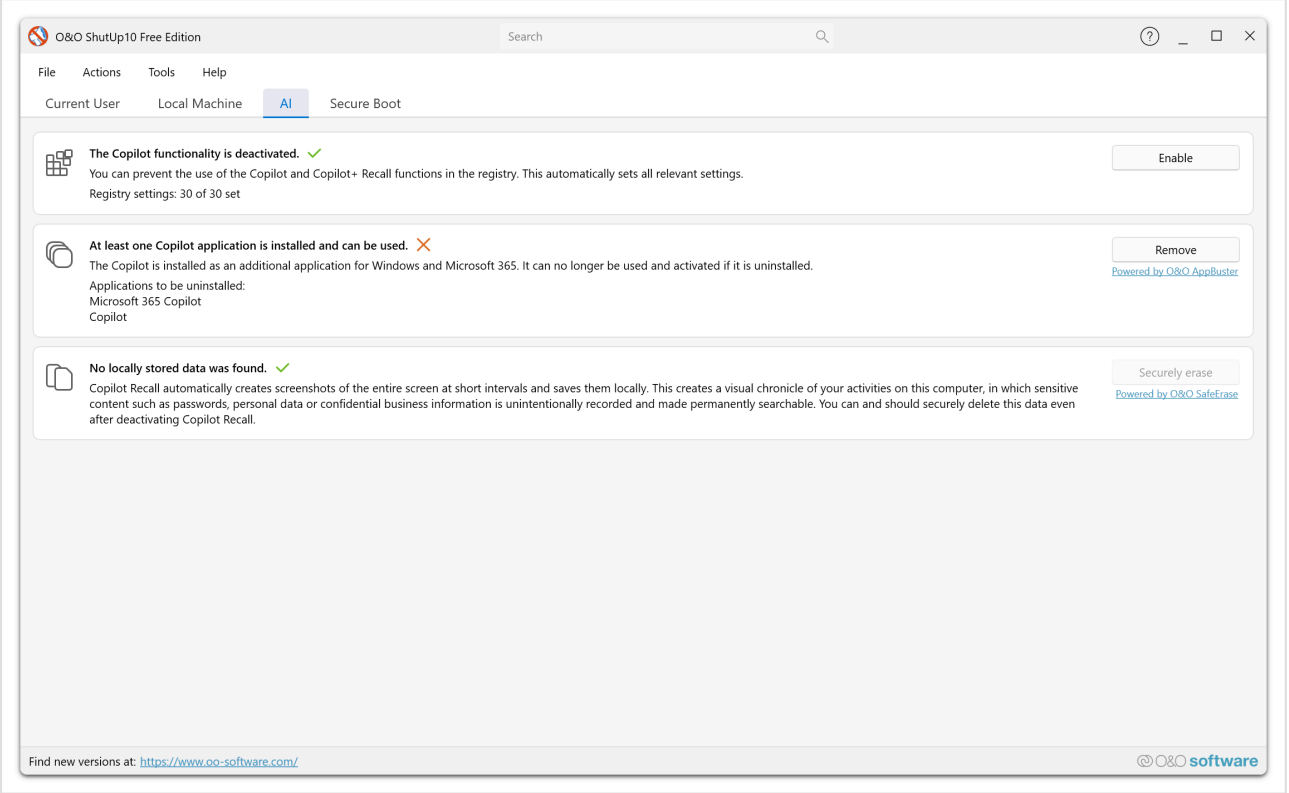
- The service continuously monitors and re-applies your configuration after Windows updates, Group Policy changes, or registry modifications.
- Open the client at any time to check the **Premium Overview** for current protection status.
- Use the Profiles Editor to create and manage custom profiles for different scenarios.

> **Tip**
>
> If the Premium Overview remains in Setup Mode after installation, verify that the O&O ShutUp10 service is running. Check **Windows Services** (services.msc) or contact your IT administrator.

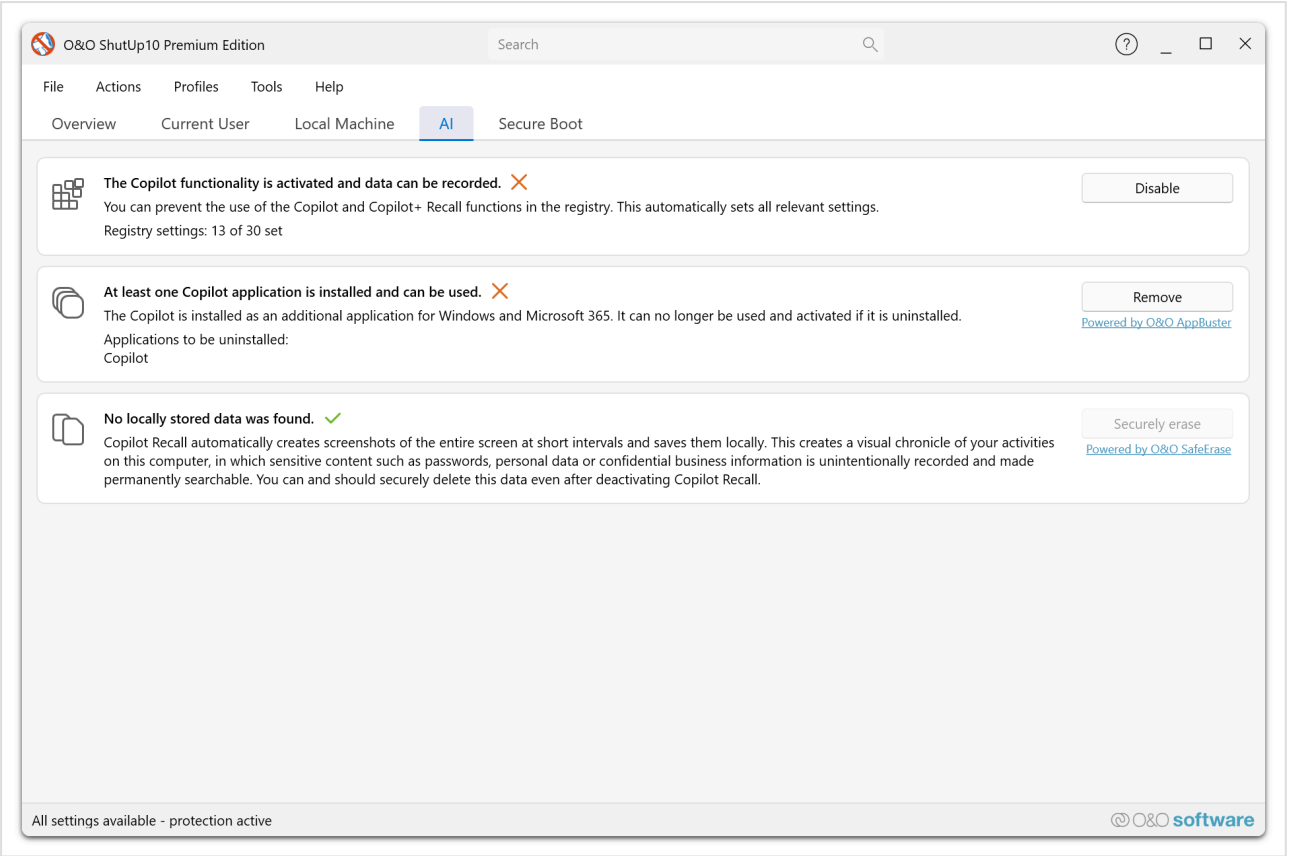
AI Removal

The AI Removal feature provides a comprehensive, three-layer approach to removing Microsoft Copilot and Recall components from your system. It is accessible from the **AI** tab in the main window and combines the O&O ShutUp10 settings engine, the O&O AppBuster engine, and the O&O SafeErase engine into a single workflow.

Free Edition:



Premium Edition:



Windows Copilot+ Recall automatically captures screenshots of your activity at regular intervals, stores them locally, and uses AI to make that history searchable. The AI Removal feature lets you address every layer of this functionality: the registry settings that enable it, the applications that power it, and the data it has already stored on your device.

AI Settings

The first layer controls the Windows registry settings that govern Copilot and AI functionality. These are a **bundle of the regular O&O ShutUp10 privacy settings** from the **Microsoft Copilot (in Windows)** category, presented together for convenience.

What the settings control

Setting	Effect
Disable the Windows Copilot	Fully disables the Copilot AI assistant in Windows.
Disable Recall enablement	Prevents Copilot+ Recall from being activated on your device.
Disable AI data analysis	Stops Windows from using AI to analyze your data locally.
Disable the Copilot button from the taskbar	Removes the Copilot button from the Windows taskbar.
Disable the Image Creator in Microsoft Paint	Disables AI-powered image generation in Paint.
Disable the Cocreator in Microsoft Paint	Disables the AI-powered Cocreator feature in Paint.
Disable AI-powered image fill in Microsoft Paint	Disables AI-powered generative fill in Paint.

How it works

- The AI tab displays a status showing how many AI-related settings are currently disabled (e.g., "5 of 8 disabled").
- Click **Disable** to apply all recommended AI settings at once.
- These settings modify the Windows registry in the same way as toggling them individually in the main settings list.

Because these are standard O&O ShutUp10 registry settings, they can be **re-enabled at any time** — either by toggling individual settings back in the main settings list, or by re-running the AI settings with the opposite configuration.

> **Tip**
>
> If you only want to disable Copilot and Recall without removing applications or data, applying the AI settings alone is sufficient and fully reversible.

AI App Removal (O&O AppBuster)

The second layer removes Copilot-related applications from your system using the **O&O AppBuster engine**. This detects and uninstalls Microsoft Copilot+ applications that are installed as Windows Store apps.

What it does

- Scans your system for installed Copilot+ applications (both per-user and machine-wide installations).
- Displays the names of any detected Copilot applications.
- Removes the applications when you click **Remove**.

Detection

The AI tab shows the current status:

Status	Meaning
Applications listed by name	One or more Copilot+ apps are installed on your system.
"No Copilot applications were found"	No Copilot+ apps are currently installed.

> **Danger**
>
> **Warning — This action cannot be undone by the application**
>
> Removing Copilot+ applications is a **permanent, one-way operation** within O&O ShutUp10. Once the applications are uninstalled, they cannot be reinstalled by this application. To restore them, you would need to reinstall them manually through the Microsoft Store or by resetting Windows components.

Secure Deletion of Recall Data (O&O SafeErase)

The third layer securely deletes the data that Copilot+ Recall has already stored on your device, using the **O&O SafeErase engine**.

What is stored in the Recall folder

Windows Copilot+ Recall stores its data in the `CoreAIPlatform.00` folder within your local application data directory (`%LOCALAPPDATA%\CoreAIPlatform.00`). This folder contains:

- **Screenshots** — Periodic captures of your screen activity taken at regular intervals.
- **OCR text data** — Extracted text from the captured screenshots, used to make your activity searchable.
- **Index databases** — Search indexes that allow Recall to find and display past activity.
- **AI model data** — Local AI processing artifacts used for on-device analysis.

This data can contain highly sensitive information: passwords visible on screen, private messages, financial data, personal documents, and anything else that was displayed on your screen while Recall was active.

How it works

- The AI tab scans the Recall data folder and reports the number of files and directories found, along with their total size.
- If no Recall data exists, the status shows **"No locally stored data was found."**
- Click **Remove completely** to securely erase all detected Recall data.

The secure deletion uses the O&O SafeErase engine, which overwrites file contents before deletion, ensuring the data cannot be recovered using file recovery tools.

> **Danger**
>
> **Warning — This action cannot be undone in any way**
>
> Secure deletion with O&O SafeErase is **permanent and irreversible**. Unlike standard file deletion (where data may remain recoverable on disk), secure erasure overwrites the file contents with random data before removing them. Once the Recall data is securely erased, it cannot be recovered by any means — not by O&O ShutUp10, not by Windows, and not by any data recovery tool.
>
> Only proceed if you are certain you no longer need any of the data stored by Recall.

Complete AI Removal

For maximum protection, you can execute all three layers together in a single operation. When you choose to deactivate all components, a confirmation dialog asks:

> "Are you sure you want to disable all components?"

Confirming this will:

1. **Disable** all AI-related registry settings (reversible).
2. **Remove** all detected Copilot+ applications (not reversible by the application).
3. **Securely erase** all Recall data stored on the device (permanently irreversible).

Status Overview

The Premium Edition overview tab includes an AI status indicator that provides a quick summary of your Copilot+ removal status:

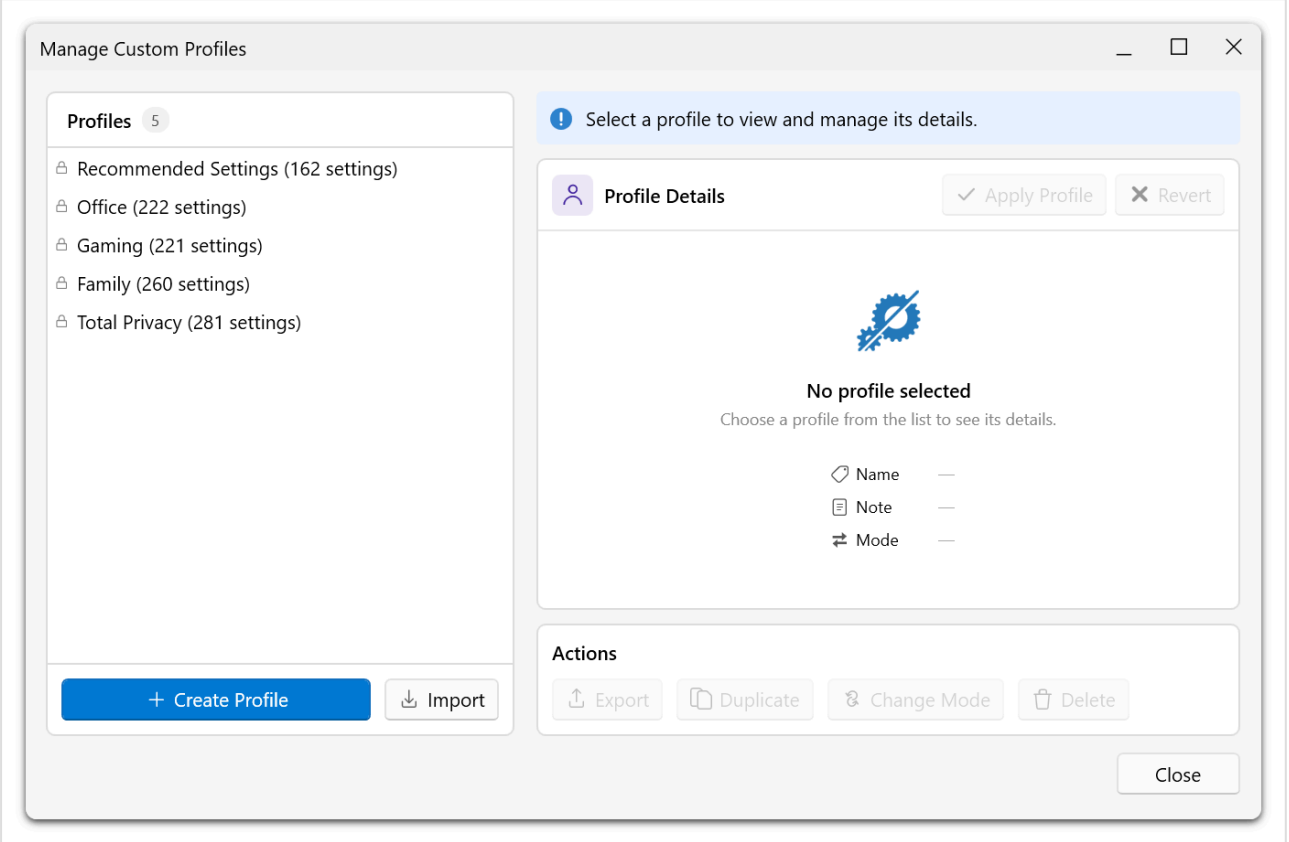
Component	Status values
Settings	"X of Y disabled"
Applications	"Not installed" or "X installed"
Recall Files	"No files detected" or "Files detected"

The overall status is shown as:

Overall status	Meaning
All Copilot+ components removed	All settings disabled, no apps installed, no Recall files.
Partially removed	Some components have been addressed, but not all.
Copilot+ components active	No removal actions have been taken.

Profiles & Export

O&O ShutUp10 supports saving and loading privacy setting profiles. This feature is available in both the Free and Premium Editions, with additional capabilities in the Premium Edition.



Overview

Profiles allow you to save your current privacy configuration and re-apply it later. This is useful for maintaining consistent settings across reinstallations, sharing configurations, or switching between different privacy levels.

Capabilities

Save Profiles

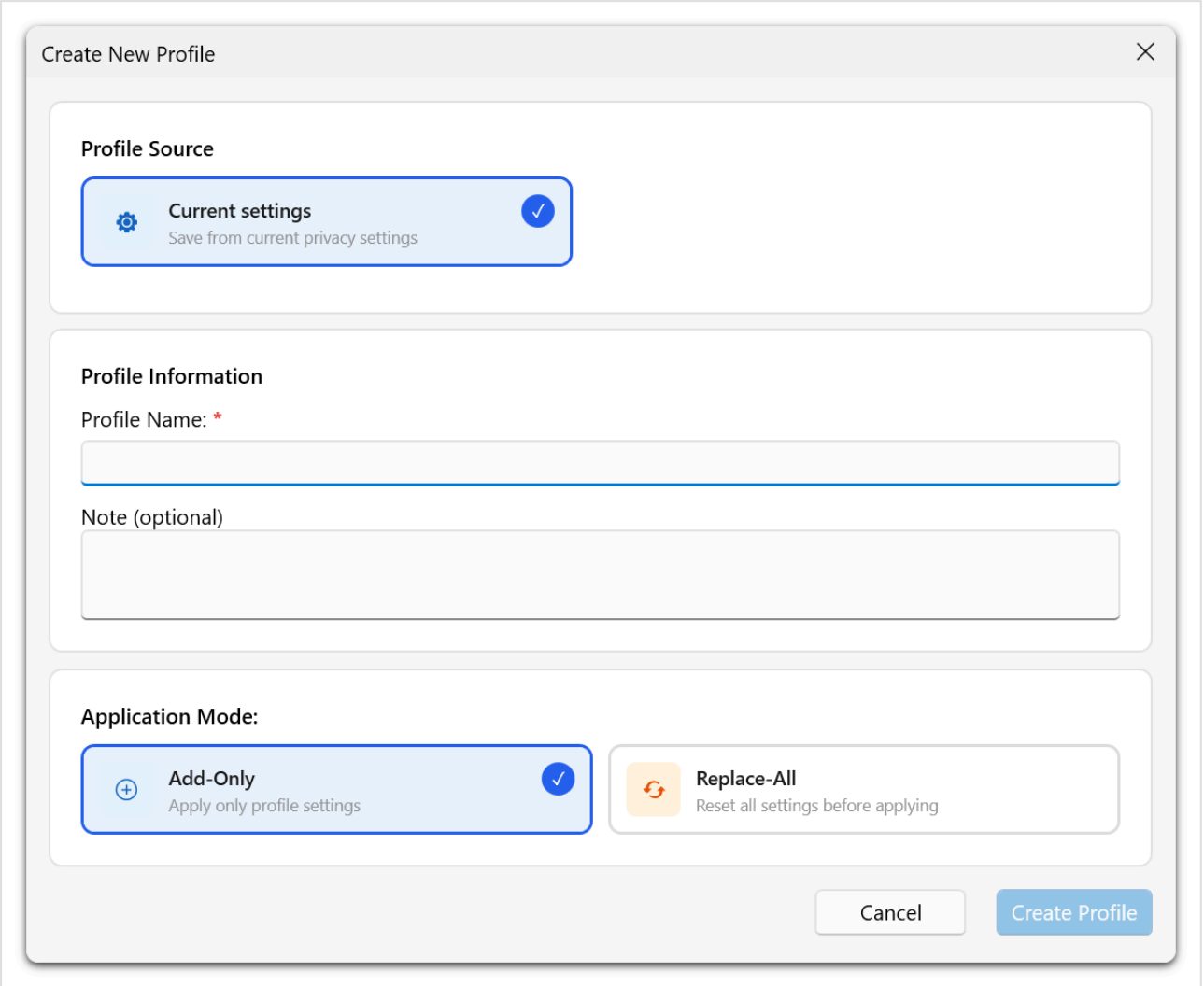
Save your current set of privacy settings as a named profile. You can create multiple profiles for different scenarios (e.g., a strict privacy profile and a balanced profile).

Load Profiles

Load a previously saved profile to instantly apply its privacy settings. This is particularly useful after a fresh Windows installation or a major Windows update.

Export and Import

Export your privacy configuration as a file that can be shared with others or transferred to another machine. Import a configuration file to apply someone else's privacy settings.



Command-Line Support

O&O ShutUp10 supports command-line parameters for applying profiles, enabling automation and integration with deployment scripts.

> **Tip**
>
> Save a profile of your preferred settings before any major Windows update. If the update resets your privacy settings, you can quickly restore them by loading your saved profile.

Profile File Structure

O&O ShutUp10++ stores profiles as configuration files that contain all your saved privacy settings. This page explains how profile files are structured and what each attribute means, so you can understand, review, or manually edit your exported profiles.

File Format

Profile files use the **INI format** — a simple text-based format with sections and key-value pairs. You can open and inspect them with any text editor (e.g., Notepad).

A profile file consists of two sections: `[Profile]` (metadata about the profile) and `[Settings]` (the actual privacy settings).

Example Profile File

```
[Profile]
Id=a3f8b2c1-4d5e-6f7a-8b9c-0d1e2f3a4b5c
Name=My Privacy Profile
Description=Balanced privacy settings for daily use
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
```

Profile Attributes

`[Profile]` Section

The `[Profile]` section contains metadata that identifies and describes the profile.

Attribute	Description	Example
Id	A unique identifier (GUID) for the profile. Automatically generated when the profile is created.	`a3f8b2c1-4d5e-6f7a-8b9c-0d1e2f3a4b5c`
Name	The display name of the profile. Must be unique across all your profiles.	`My Privacy Profile`
Description	An optional note or description explaining the purpose of the profile.	`Balanced privacy settings for daily use`
Created	The date and time when the profile was first created (ISO 8601 format).	`2025-03-15T10:30:00Z`
Modified	The date and time when the profile was last modified (ISO 8601 format).	`2025-04-01T14:22:00Z`
IsSystem	Indicates whether this is a built-in system profile (`true`) or a user-created profile (`false`).	`false`
Icon	The icon associated with the profile in the application UI.	`custom`

`[Settings]` Section

The `[Settings]` section contains the actual privacy settings as key-value pairs. Each entry represents one privacy setting controlled by O&O ShutUp10++.

Component	Description	Example
Key	The internal name of the privacy setting.	`DisableTelemetry`
Value	The desired state for that setting (`true` = privacy protection enabled, `false` = Windows default).	`true`

The settings correspond to the same options you see in the O&O ShutUp10++ user interface. Only settings that are explicitly configured are included in the file — settings not listed in the profile are left unchanged when the profile is applied.

Profile Types

Built-in (System) Profiles

These profiles are provided by O&O ShutUp10++ and are always available:

- Cannot be modified or deleted
- Updated automatically with application updates
- Always apply settings in **Add-Only** mode (only changes settings that are not already configured)
- Identified by `IsSystem=true` in the file

User-Created (Custom) Profiles

These are profiles you create yourself:

- Can be created, renamed, edited, deleted, exported, and imported
- Can use either **Add-Only** or **Replace-All** application mode

- Identified by `IsSystem=false` in the file
- Stored alongside your user settings

Application Modes

When applying a profile, O&O ShutUp10++ supports two modes:

Mode	Behavior
Add-Only	Only applies settings from the profile that do not conflict with your current configuration. Existing settings are not overwritten.
Replace-All	Overwrites all current settings with the values defined in the profile. Settings not included in the profile are reset to Windows defaults.

Built-in profiles always use Add-Only mode. For custom profiles, you can choose which mode to use when applying.

Exporting and Sharing Profiles

When you export a profile, the resulting file contains the complete `[Profile]` and `[Settings]` sections as described above. You can:

- Share the file with other users or machines
- Back up profiles before a Windows update
- Manually edit the file to adjust settings before importing

> **Tip**
>
> After exporting a profile, open the file in a text editor to review exactly which settings are included and what values they are set to.

FAQ

- **Can I edit a profile file manually?** Yes, profile files are plain text. You can open them in any text editor to review or modify settings before importing.
- **What happens if I change the Id?** The application uses the Id to identify profiles. Changing it will cause the file to be treated as a new profile on import.
- **Do profile names have to be unique?** Yes. If you import a profile with a name that already exists, you will be asked to rename it.
- **What happens to settings not listed in the profile?** They are left unchanged when using Add-Only mode, or reset to Windows defaults when using Replace-All mode.
- **Are profiles portable between machines?** Yes. You can export a profile from one machine and import it on another running O&O ShutUp10++.

Edit Mode

Edit Mode provides a safe way to preview and batch multiple privacy setting changes before applying them to your system. It is available in both the Free and Premium Editions.

Motivation

By default, toggling a privacy setting in O&O ShutUp10 applies the change immediately to the Windows registry. While this is convenient for individual adjustments, it can be risky when making many changes at once — especially if a particular combination of settings causes unexpected behavior.

Edit Mode solves this by **buffering** all changes instead of applying them immediately. You can review your intended changes, apply them all at once, save them as a custom profile (Premium only), or discard them entirely. This makes Edit Mode the safest way to experiment with privacy configurations.

How It Works

Enabling Edit Mode

1. Open the **Edit** menu in the main window.
2. Click **Enable Edit Mode**.

When Edit Mode is active:

- A notification banner appears at the top of the settings list indicating that Edit Mode is active and changes are buffered.
- The banner displays the number of buffered changes (e.g., "5 buffered").
- Settings you toggle are highlighted but **not yet applied** to the system.

Making Changes

While Edit Mode is active, toggle any privacy settings as you normally would. Each change is stored in a buffer rather than being written to the registry. You can freely toggle settings on and off without any immediate system impact.

Applying Buffered Changes

When you are satisfied with your changes:

1. Open the **Edit** menu and click **Apply**, or click the **Apply** button on the Edit Mode banner.
2. A confirmation dialog shows the number of buffered changes and asks for confirmation.
3. All buffered changes are applied to the system at once.

Discarding Buffered Changes

If you want to discard all buffered changes without applying them:

1. Open the **Edit** menu and click **Discard**, or click the **Discard** button on the Edit Mode banner.
2. A confirmation dialog asks you to confirm discarding the changes.
3. All buffered changes are removed and the settings return to their previous states.

Disabling Edit Mode

When you disable Edit Mode (by clicking **Enable Edit Mode** again to toggle it off), the application checks for unapplied buffered changes. If there are pending changes, you are prompted to either apply or discard them before Edit Mode is deactivated.

Saving Changes as a Profile Premium

In the Premium Edition, you can save your buffered changes as a reusable custom profile:

1. Enable Edit Mode and configure your desired settings.
2. Open the **Edit** menu and click **Save Custom Profile**.
3. Enter a profile name and optional description.
4. The buffered changes are saved as a named profile that can be re-applied later through the Profiles Editor.

This workflow is the primary way to create custom profiles — it ensures that only your intentional changes are captured in the profile.

Advantages of Edit Mode

Benefit	Description
Safety	No changes are applied until you explicitly confirm, reducing the risk of unintended system modifications.
Batch operations	Apply multiple related changes simultaneously instead of one at a time.
Preview before commit	Review the full set of intended changes before any take effect.
Easy rollback	Discard all buffered changes with a single action if you change your mind.
Profile creation	Save your curated set of changes as a reusable profile (Premium only).

> **Tip**
>
> Use Edit Mode whenever you plan to change more than a few settings at once. It provides a safety net that prevents accidental modifications and lets you review the full impact of your changes before committing them.

Settings Dialog

The Settings Dialog centralizes all application configuration options in a single, tabbed interface. It is accessible from **View** → **Settings…** in the main menu.

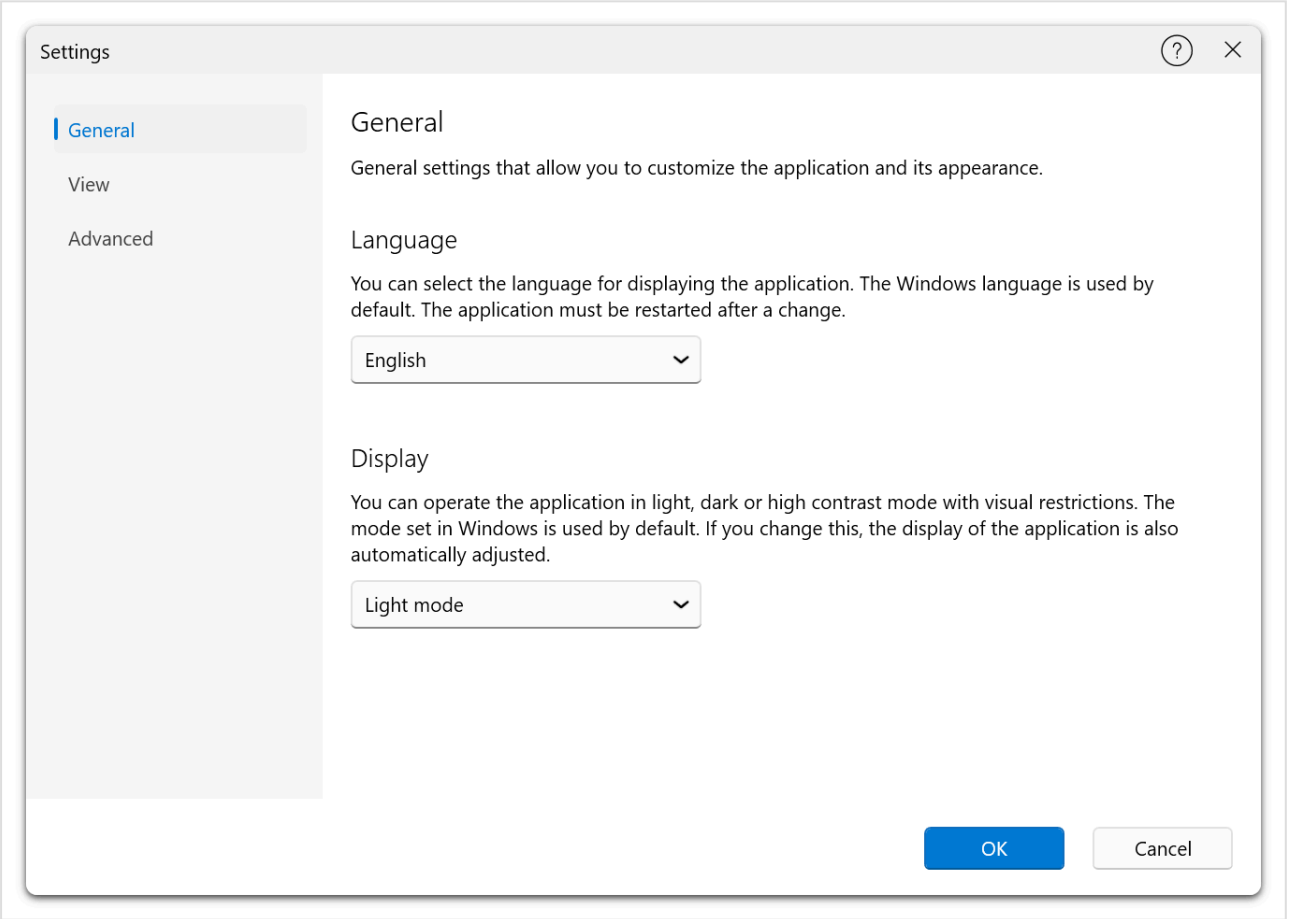
Overview

The Settings Dialog replaces the previously scattered configuration options that were available across different menus. All changes are persisted immediately when you click **OK**, and visual changes (theme, color scheme) are applied in real time.

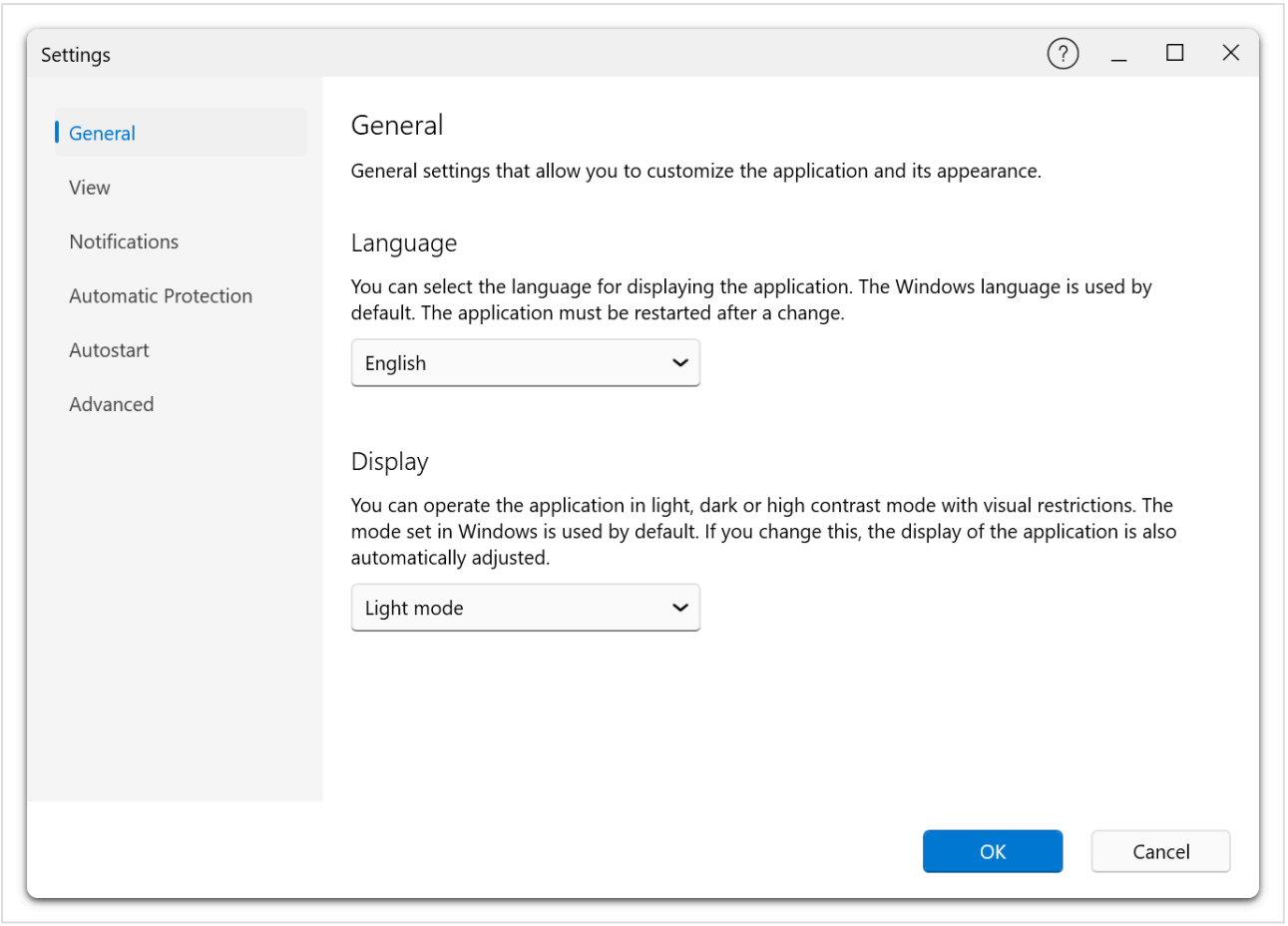
General Tab

General settings that you can use to customize the application and its appearance.

Free Edition:



Premium Edition:



Language

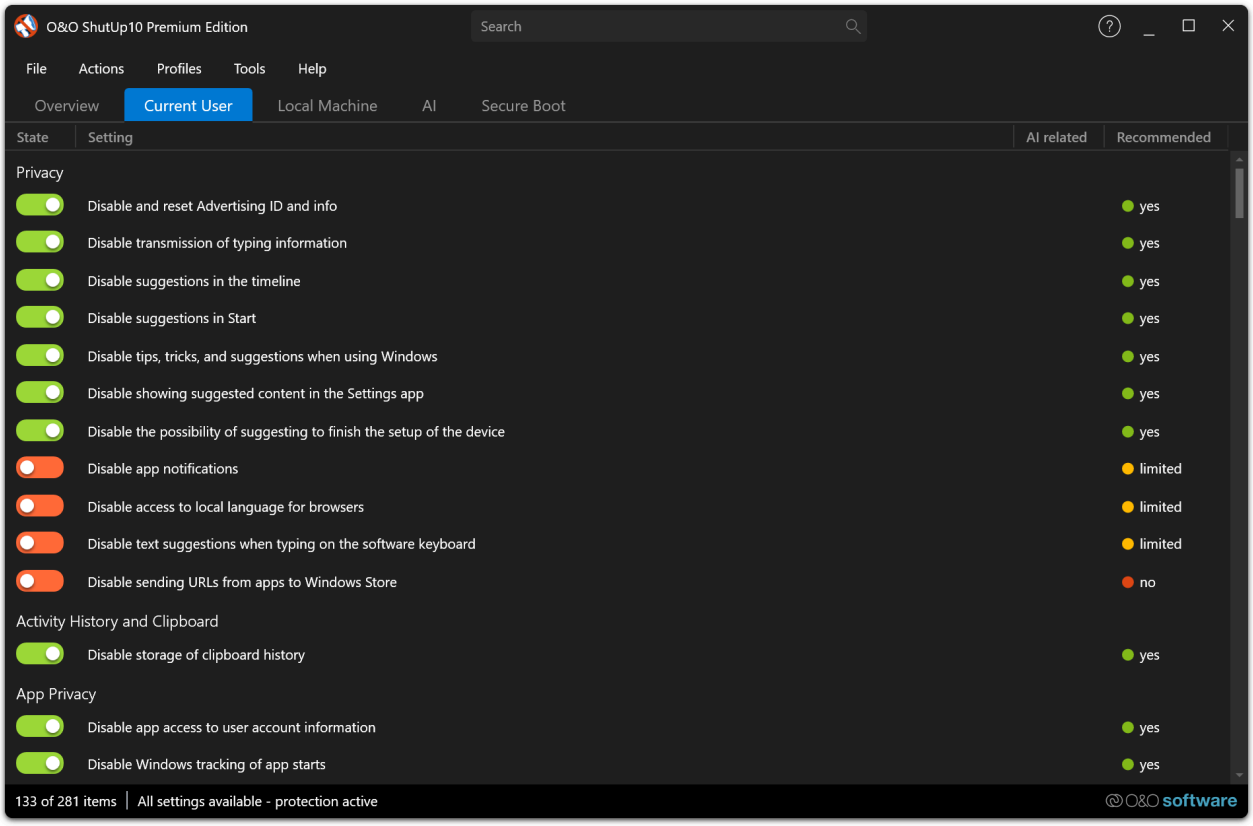
Select the display language for the application. Available languages include English (default), German, Spanish, French, Italian, Japanese, Russian, and Chinese. Changing the language requires an application restart.

App View Mode

Choose the application theme:

Option	Description
System	Follows the current Windows theme (light or dark).
Light	Forces a light appearance.
Dark	Forces a dark appearance.
High Contrast Black	High-contrast theme with a black background for accessibility.
High Contrast White	High-contrast theme with a white background for accessibility.

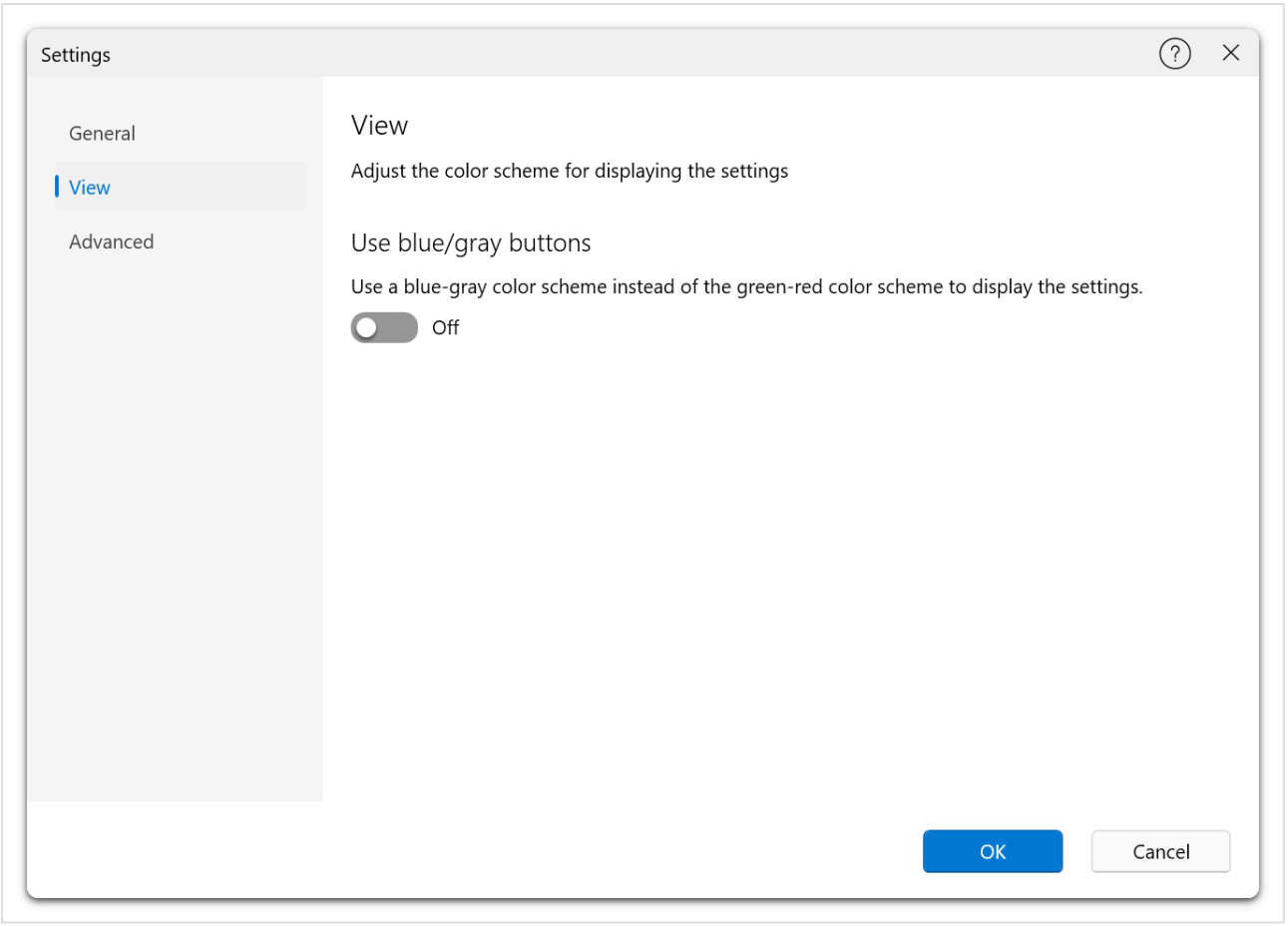
Theme changes are applied immediately without restarting the application.



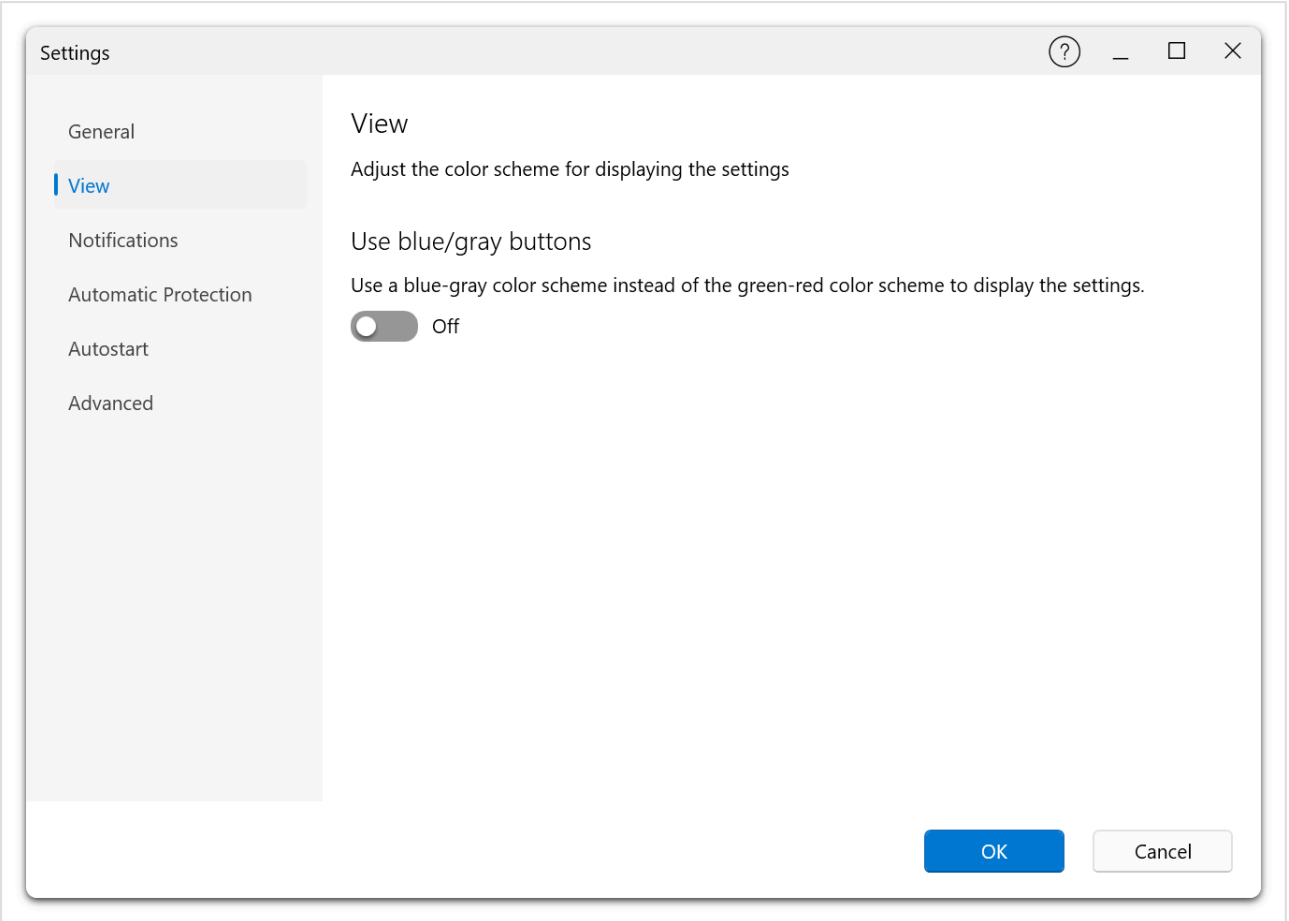
View Tab

Adjust the color scheme for displaying the settings.

Free Edition:



Premium Edition:



Use Blue/Gray Buttons

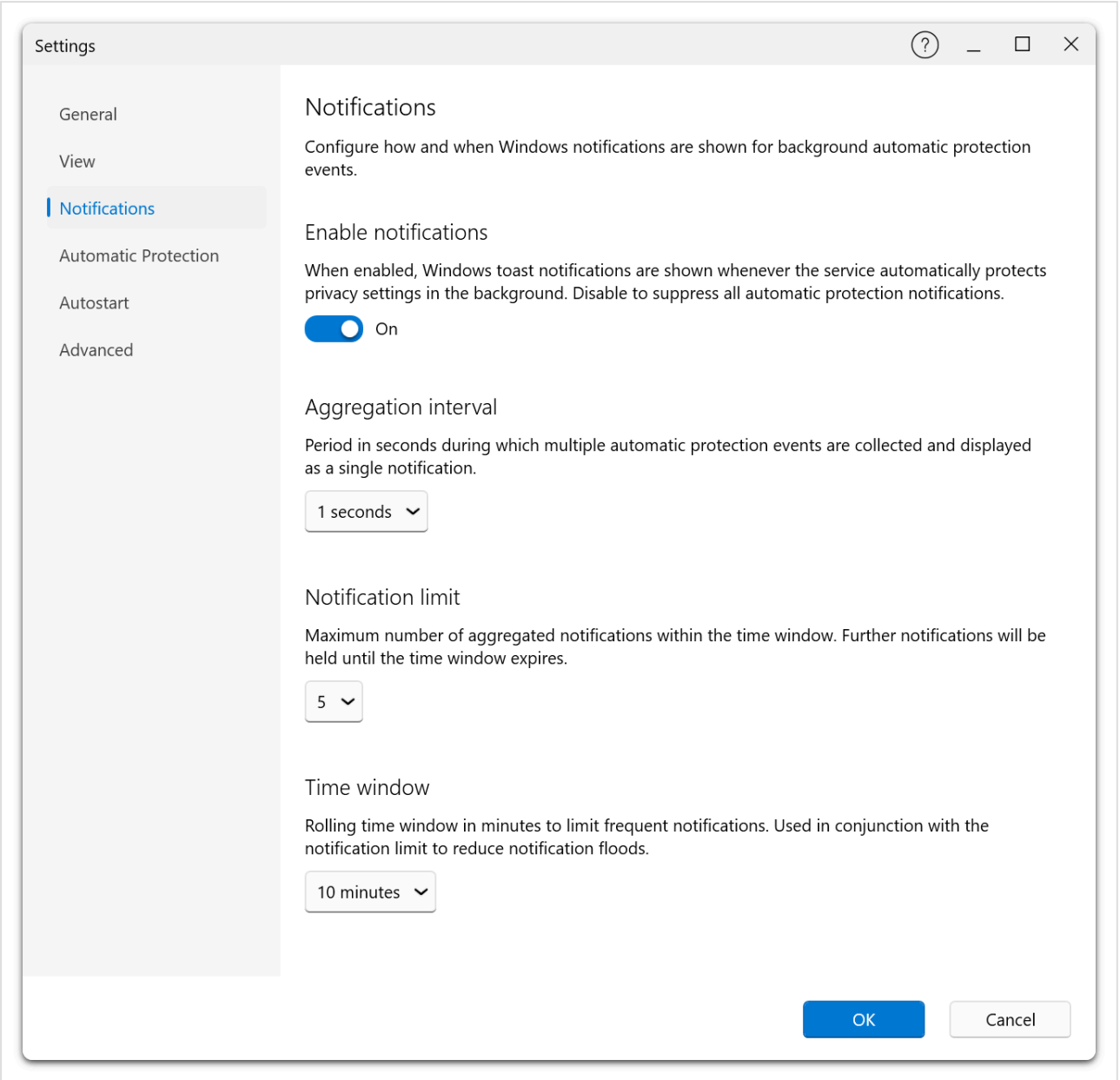
Toggle between two color schemes for the settings toggle switches:

- **Green/Red** (default) — Green indicates an active (privacy-protecting) setting; red indicates an inactive setting.
- **Blue/Gray** — A neutral color scheme using blue and gray tones.

The color scheme change is applied in real time.

Notifications Tab Premium

Configure how and when Windows notifications are shown for background automatic protection events.



This tab is only available in the Premium Edition and requires the background service to be running. If the service is not available, a warning message is displayed and the controls are disabled.

Enable Notifications

When enabled, Windows toast notifications are shown whenever the service automatically protects privacy settings in the background. Disable to suppress all automatic protection notifications.

Aggregation Interval

Defines how long the service waits (in seconds) before sending a combined notification for multiple events. Available values: 1, 2, 5, 10, 15, 30, 60, or 120 seconds.

Suppression Threshold

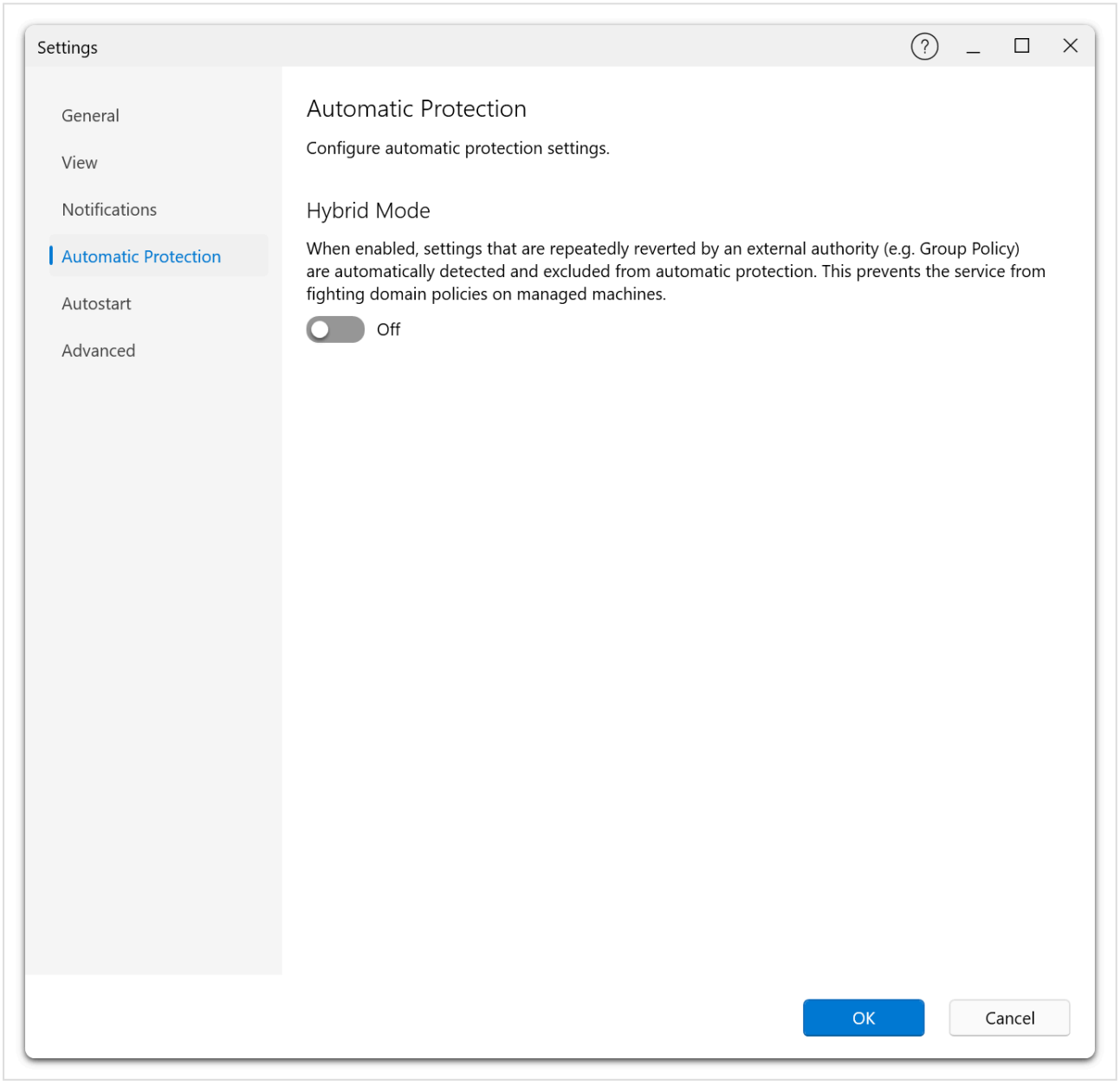
Maximum number of notifications allowed within the suppression window before further notifications are suppressed. Available values: 1, 2, 3, 5, 10, 15, or 20.

Suppression Window

Rolling time window (in minutes) used together with the suppression threshold for flood prevention. Available values: 1, 2, 5, 10, 15, 30, or 60 minutes.

Automatic Protection Tab Premium

Configure automatic protection settings.



This tab is only available in the Premium Edition and requires the background service to be running.

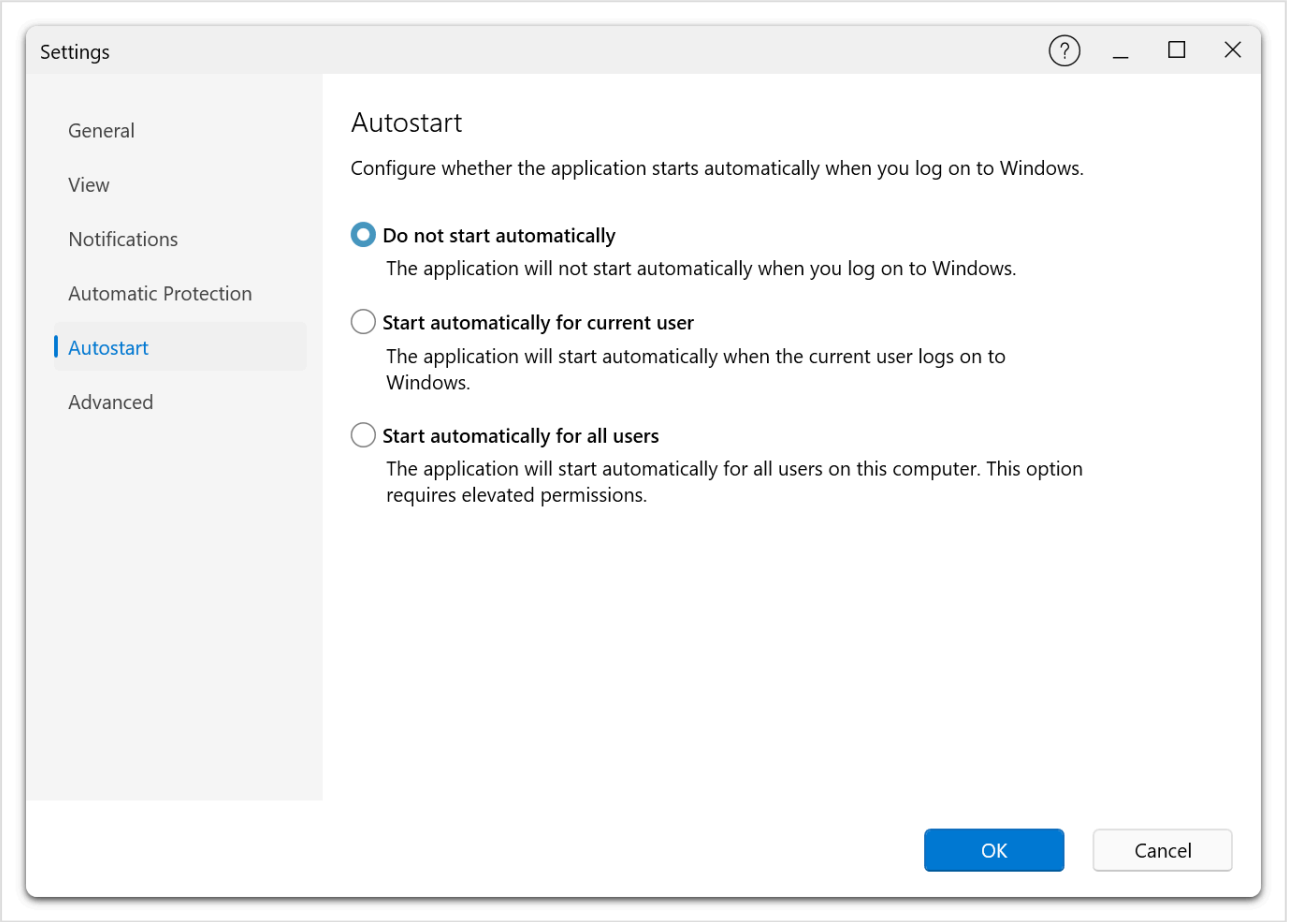
Hybrid Mode

When enabled, settings that are repeatedly reverted by an external authority (e.g., Group Policy) are automatically detected and excluded from automatic protection. This prevents the service from fighting domain policies on managed machines.

Hybrid Mode is particularly useful in corporate environments where certain privacy settings are controlled by organizational Group Policy and should not be overridden by the ShutUp10 service.

Autostart Tab Premium

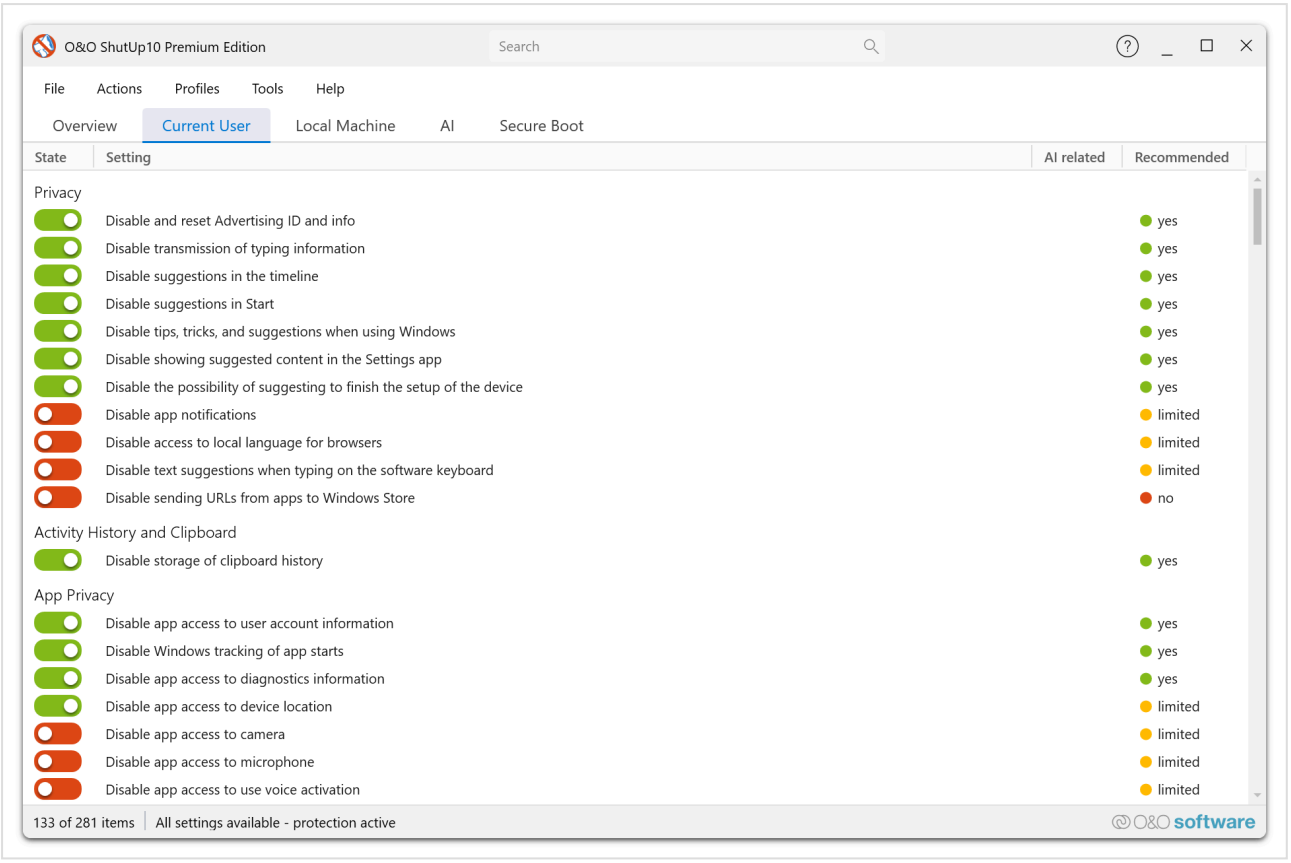
Configure whether the application starts automatically when you log on to Windows.

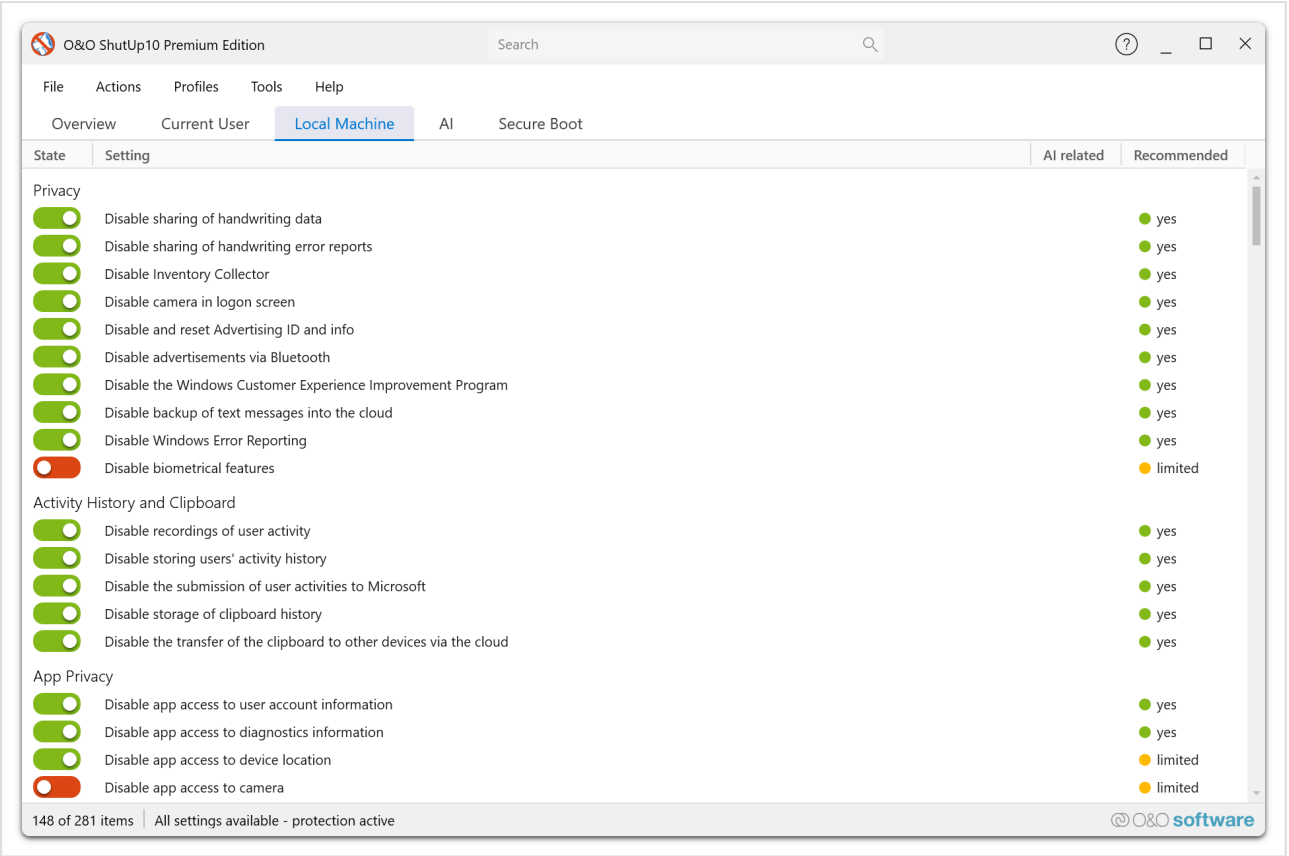


This tab is only available in the Premium Edition.

Option	Description
Do not start automatically	The application will not start automatically when you log on to Windows.
Start automatically for current user	The application starts automatically when the current user logs on.
Start automatically for all users	The application starts automatically for all users on the computer. Requires elevated permissions.

The following examples illustrate the autostart options as they appear in the client interface:

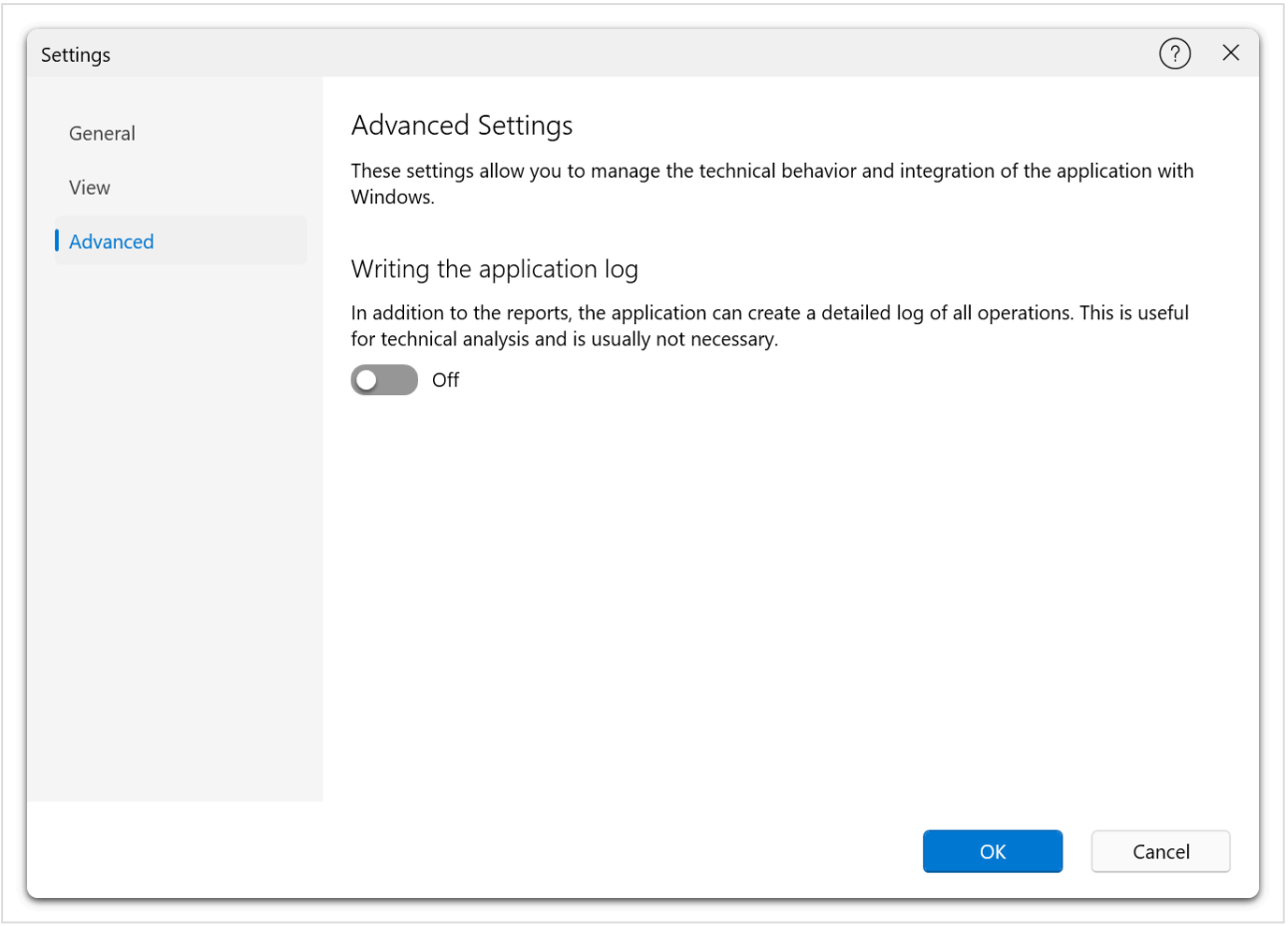

O&O ShutUp10 Premium Edition
Search
File
Actions
Profiles
Tools
Help
Overview
Current User
Local Machine
AI
Secure Boot
State
Setting
AI related
Recommended
Privacy
Disable and reset Advertising ID and info
yes
Disable transmission of typing information
yes
Disable suggestions in the timeline
yes
Disable suggestions in Start
yes
Disable tips, tricks, and suggestions when using Windows
yes
Disable showing suggested content in the Settings app
yes
Disable the possibility of suggesting to finish the setup of the device
yes
Disable app notifications
limited
Disable access to local language for browsers
limited
Disable text suggestions when typing on the software keyboard
limited
Disable sending URLs from apps to Windows Store
no
Activity History and Clipboard
Disable storage of clipboard history
yes
App Privacy
Disable app access to user account information
yes
Disable Windows tracking of app starts
yes
Disable app access to diagnostics information
yes
Disable app access to device location
limited
Disable app access to camera
limited
Disable app access to microphone
limited
Disable app access to use voice activation
limited
133 of 281 items
All settings available - protection active
O&O software



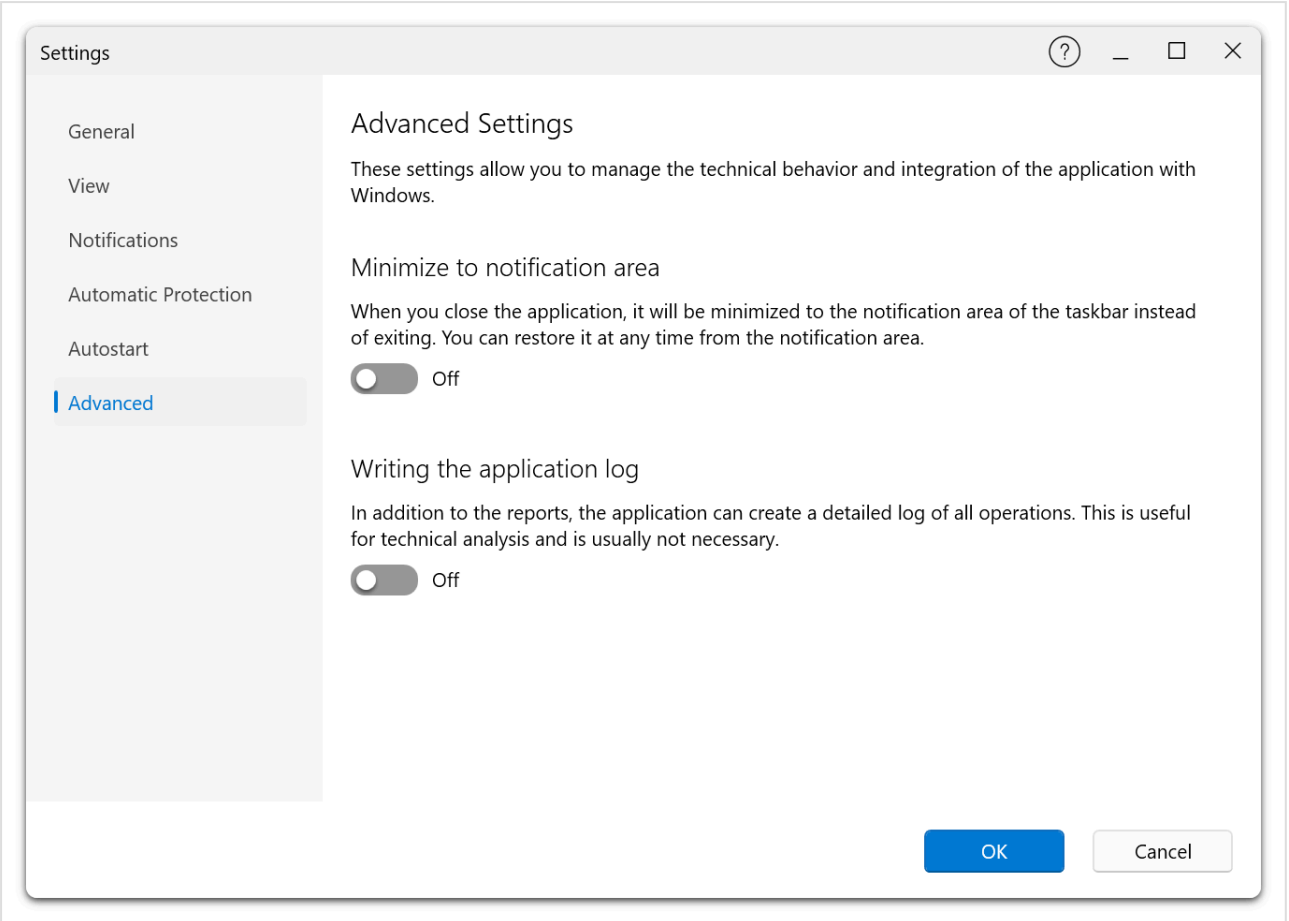
Advanced Tab

These settings allow you to manage the technical behavior and integration of the application with Windows.

Free Edition:



Premium Edition:



Minimize to Notification Area Premium

When enabled, closing the application minimizes it to the notification area (system tray) instead of exiting. You can restore it at any time from the notification area icon. This is a Premium-only feature.

Enable Logging

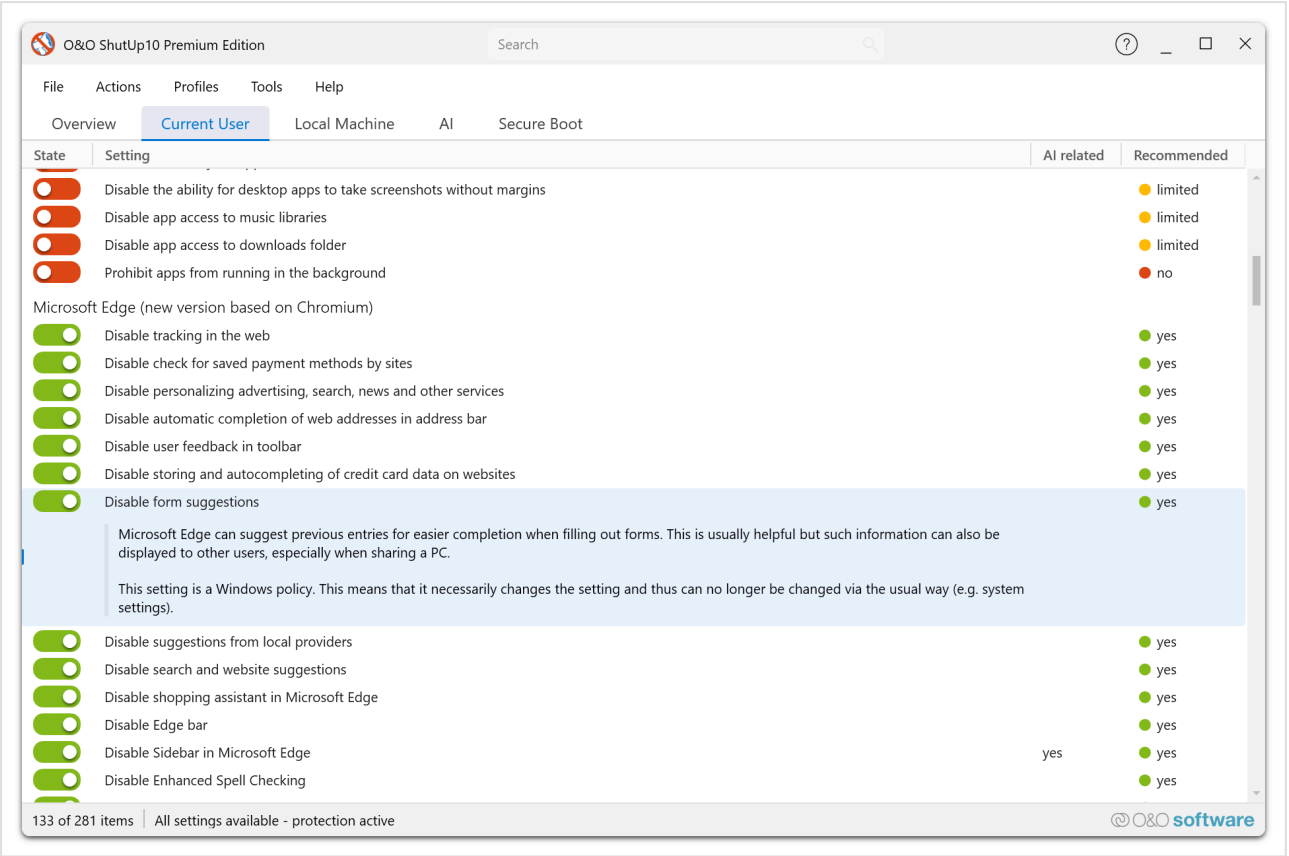
In addition to the standard reports, you can have the application create a detailed log of all operations. This is useful for technical analysis and troubleshooting. Logging is hidden in BlueCon and Fortress Mode builds.

Update Check

Configure whether the application automatically checks for new versions at startup. When enabled, the application contacts the O&O Software update server to determine if a newer version is available. If a newer version is found, a notification is displayed with an option to download the update. Disable this option if you prefer to check for updates manually or if your environment restricts outbound network access.

Information Tab

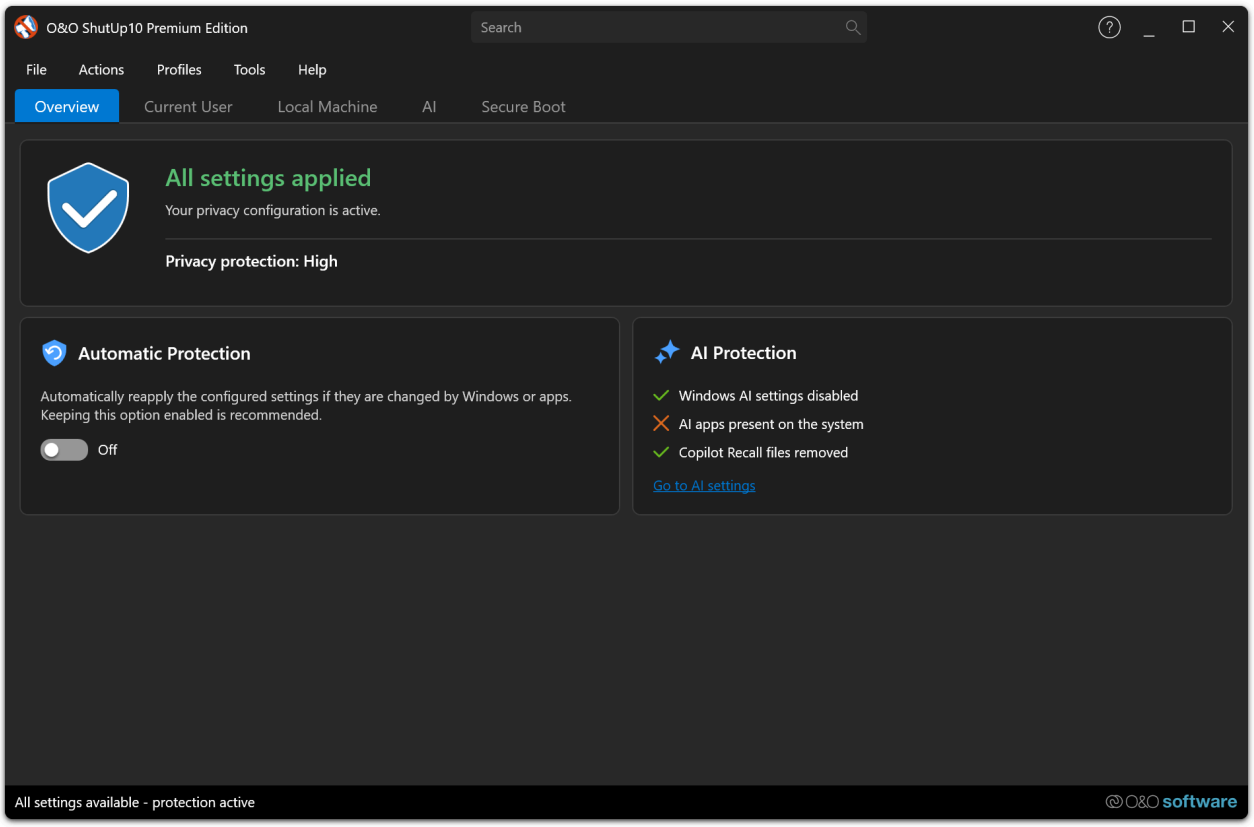
Displays version information and product details about the application.



The Information tab provides a quick reference for the installed version of O&O ShutUp10, including the edition type, build number, and copyright information. This is useful for verifying your installation when contacting support or checking compatibility.

Automatic Protection Premium

Automatic Protection is an exclusive feature of the **O&O ShutUp10 Premium Edition**. It ensures your privacy settings remain applied even after Windows updates, Group Policy changes, or other system modifications.



Overview

Windows updates frequently reset privacy settings to their defaults. In the Free Edition, users must manually re-check and re-apply their preferred settings after each update. The Premium Edition solves this with Automatic Protection.

How It Works

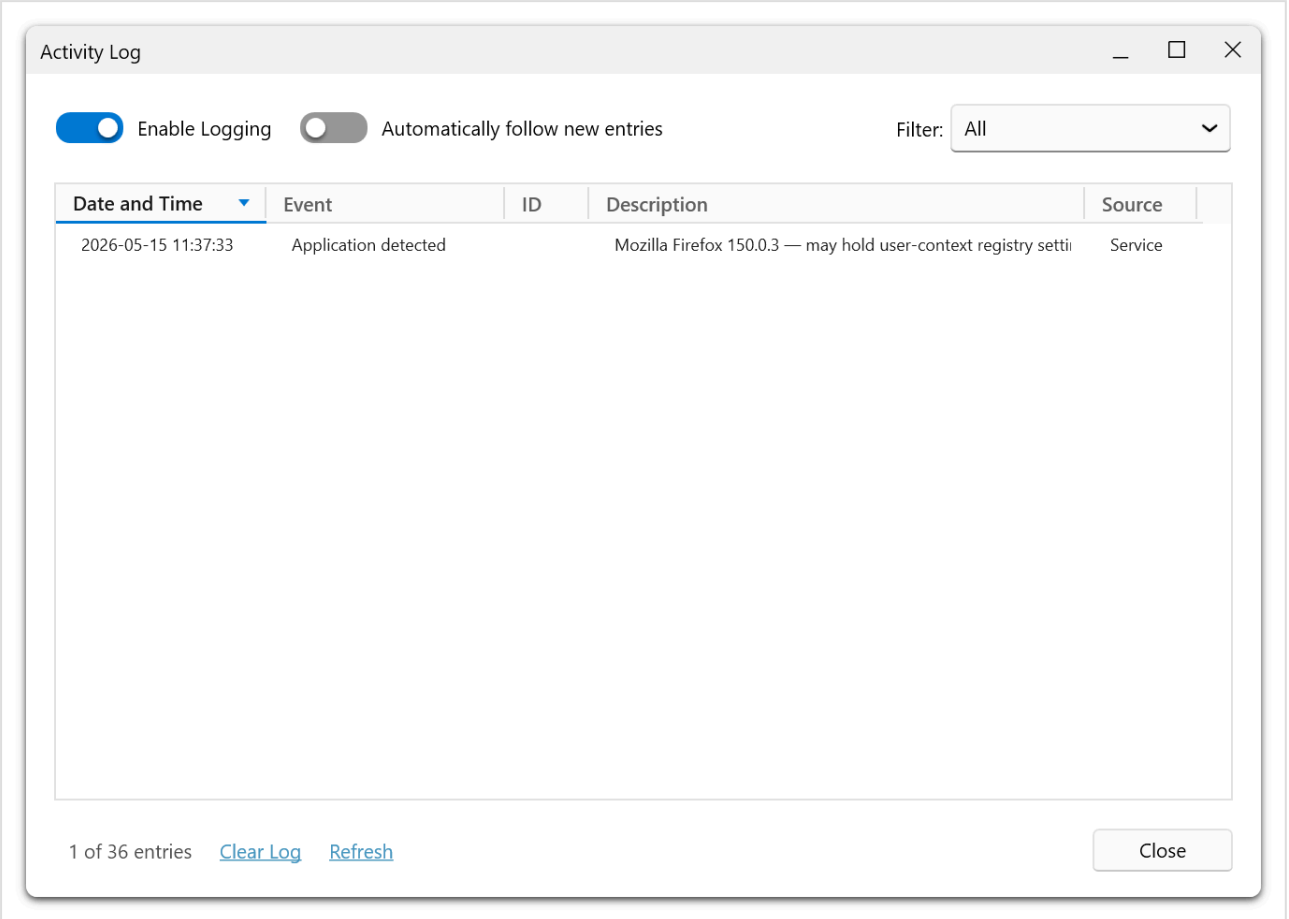
The O&O ShutUp10 service runs in the background and continuously monitors your privacy settings. When it detects a change — whether caused by a Windows update, a Group Policy push, or any other system modification — it automatically re-applies your preferred configuration.

Monitored Events

The service responds to:

- **Windows Updates** — Settings that were reset during a cumulative or feature update are restored.

- **Group Policy changes** — If a policy override conflicts with your preferences, the service re-applies your settings.
- **Registry modifications** — Direct changes to privacy-related registry values are detected and corrected.



Configuration

You configure your preferred privacy settings once through the client application. The service stores this configuration and uses it as the baseline for Automatic Protection.

> **Info**
>
> Automatic Protection requires the O&O ShutUp10 service to be running. If the service is stopped, settings will not be automatically re-applied until the service is restarted.

Benefits

- **Set-and-forget privacy** — Configure once, stay protected continuously.
- **Protection against update regressions** — Windows updates no longer silently undo your privacy choices.
- **Zero user intervention required** — The service handles everything in the background.

Profiles Editor Premium

The Profiles Editor is an exclusive feature of the **O&O ShutUp10 Premium Edition**. It provides a full management interface for creating, organizing, and applying privacy setting profiles.

Overview

Profiles allow you to save a specific set of privacy settings and re-apply them at any time. The Profiles Editor (accessible from **Profiles → Custom Profiles…** in the main menu) lets you manage both built-in default profiles and your own custom profiles.

Built-in Default Profiles

The Profiles Editor includes several built-in default profiles that provide ready-made privacy configurations for common scenarios. These profiles are read-only and cannot be modified or deleted.

Profile	Description
Recommended Settings	Enables all recommended privacy settings. Safe for most users with minimal impact on functionality.
Limited Settings	Enables all limited privacy settings. Enhanced privacy protection that may affect some Windows features.
Critical Settings	Enables all critical privacy settings. Maximum privacy protection that may significantly impact functionality.
Recommended + Limited Settings	Enables all recommended and limited privacy settings. Enhanced privacy protection that may affect some Windows features.
All Settings (Maximum Privacy)	Enables all privacy settings across recommended, limited, and critical categories. Maximum privacy protection that may significantly impact functionality.
Factory Reset	Resets all privacy settings to Windows factory defaults. Restores original system behavior.
Recommended settings by the BSI	Applies all settings recommended by the German Federal Office for Information Security (BSI) for disabling wireless technologies, telemetry, and related features in Windows 10/11.

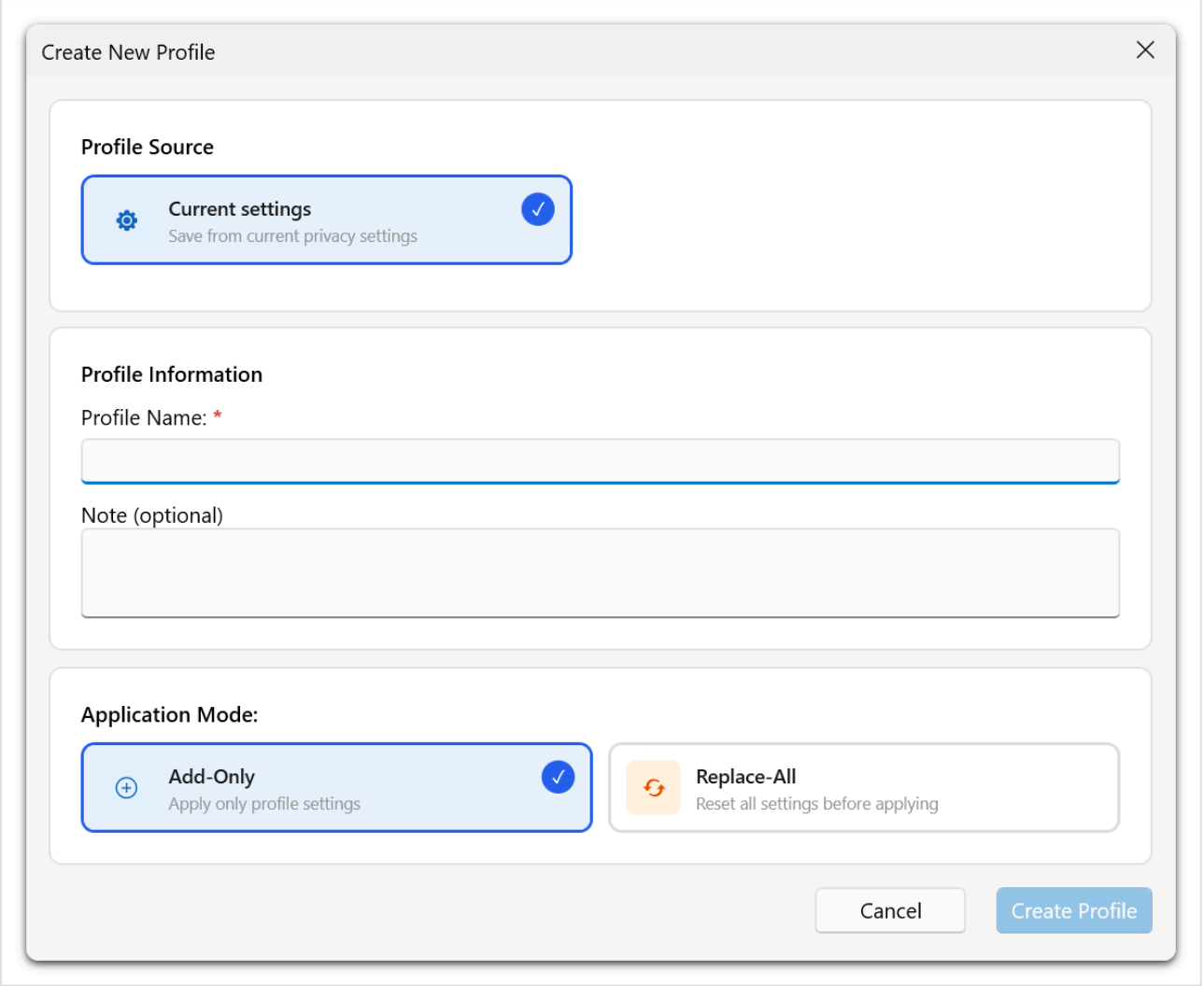
> **Caution**
>
> Built-in profiles marked as **read-only** cannot be renamed, edited, or deleted. They are maintained by the application and updated with new releases.

Creating Custom Profiles

Custom profiles are created using **Edit Mode** (see Edit Mode). The workflow is:

1. **Enable Edit Mode** from the Edit menu.
2. **Toggle settings** to configure your desired privacy state — changes are buffered and not applied immediately.
3. **Save as Profile** from the Edit menu — the Save Custom Profile dialog opens.
4. Enter a **profile name** (required) and an optional **description/note**.

5. Click **Create Profile** to save.



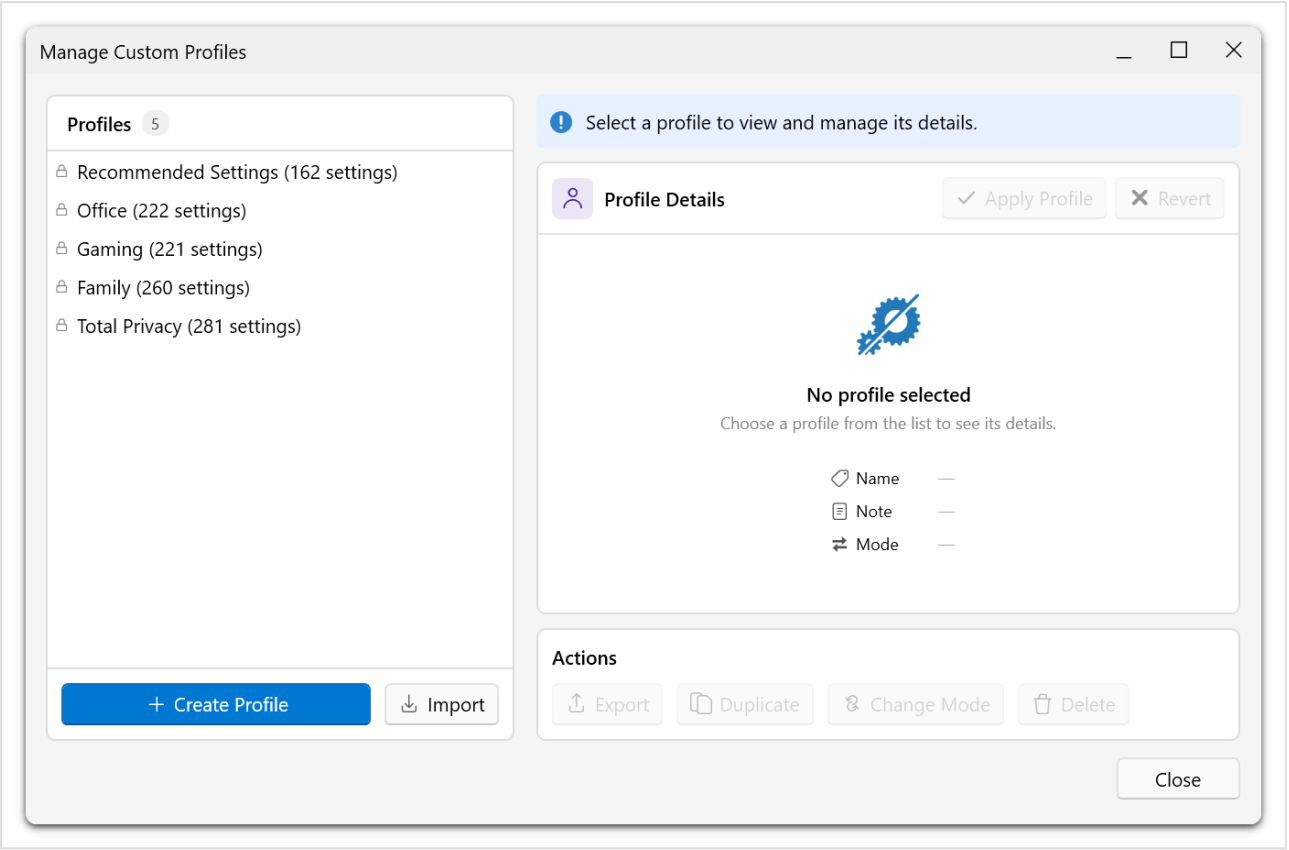
The profile stores all buffered setting changes. You can create multiple profiles for different scenarios (e.g., a strict profile for personal use and a balanced profile for a shared workstation).

Validation Rules

- A profile name is required. An empty name is not accepted.
- Duplicate profile names are not allowed.
- You must have at least one buffered change before saving.

Managing Profiles

The **Manage Custom Profiles** dialog (accessible from **Profiles** → **Custom Profiles…**) provides a two-panel interface:



Left Panel — Profile List

Displays all available profiles (built-in and custom) with a profile count header. Select a profile to view its details.

Right Panel — Profile Details and Actions

Shows the selected profile's metadata:

- **Profile name**
- **Creation date**
- **Number of settings** included in the profile
- **Note/description**

Available actions for custom profiles:

Action	Description
Apply Profile	Applies all settings from the selected profile to the system.
Rename	Change the profile name.
Edit Note	Modify the profile description.
Delete	Permanently remove the custom profile.

> **Info**
>
> Built-in default profiles only support the **Apply Profile** action. Rename, Edit Note, and Delete are not available for built-in profiles.

Applying a Profile

When you apply a profile, all privacy settings contained in that profile are applied to the system. For built-in profiles, settings are applied according to their recommendation level. For custom profiles, the exact setting states captured when the profile was created are restored.

> **Tip**
>
> Before applying a profile that changes many settings, consider creating a system restore point from the **Actions** menu. This allows you to easily revert all changes if needed.

Premium Overview Premium

The **Premium Overview** is a dual-purpose page in the O&O ShutUp10 Premium Edition that serves as both the initial setup entry point and the ongoing status dashboard. It is displayed in the main window as the primary tab when the Premium Edition is running.

Overview

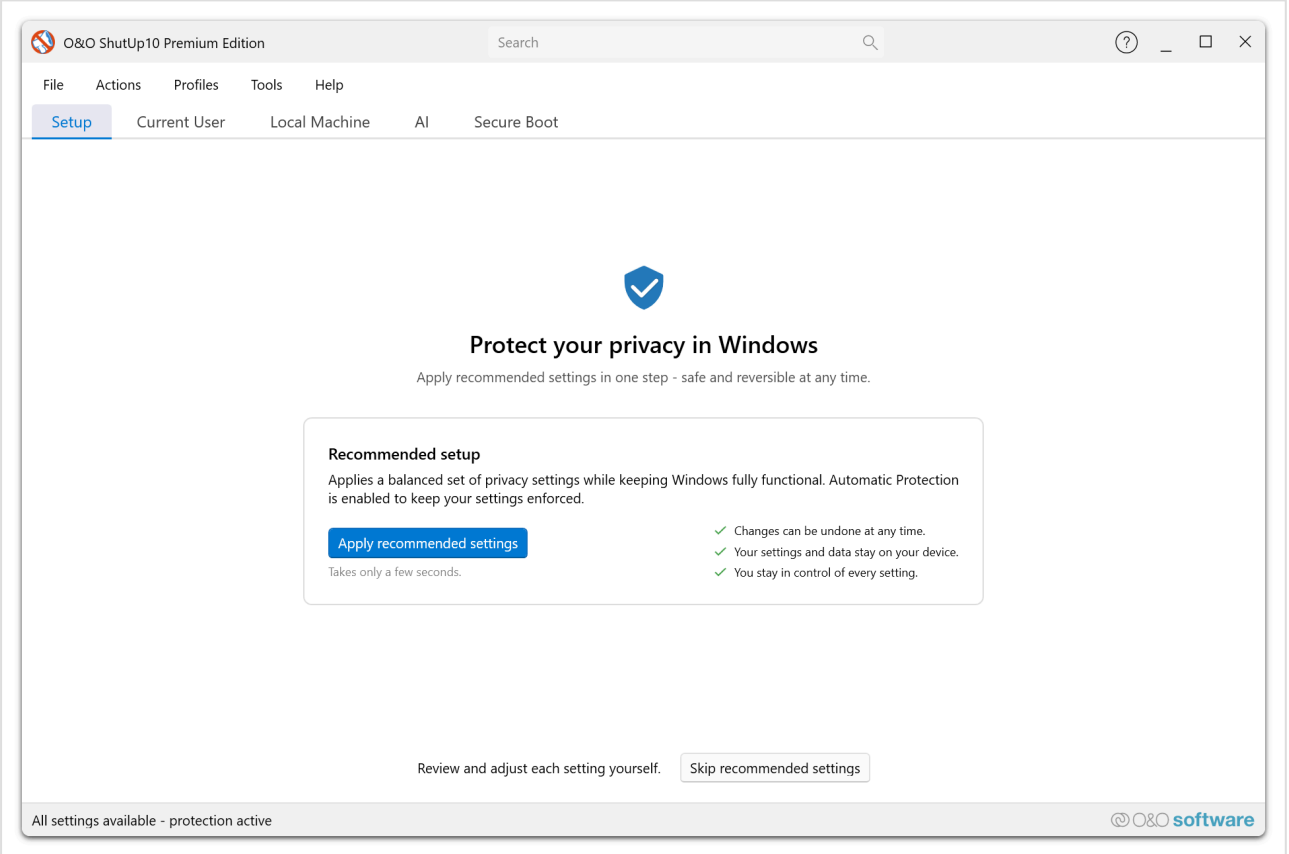
The Premium Overview operates in two distinct modes depending on the current state of the application:

- **Setup Mode** — Displayed when the Premium Edition has not yet been fully configured (e.g., after a fresh installation or when the background service is not yet connected).
- **Overview Mode** — Displayed once the initial setup is complete and the service is running, providing a real-time summary of protection status and key metrics.

The page automatically transitions from Setup Mode to Overview Mode once all required configuration steps have been completed.

Setup Mode

Setup Mode guides the user through the initial configuration of the Premium Edition after installation.



When the Premium Edition is launched for the first time — or when the background service has not yet been configured — the Premium Overview displays a guided setup workflow. This mode ensures that all prerequisites are met before automatic protection begins.

What Setup Mode Covers

Step	Description
Service Installation	Verifies that the O&O ShutUp10 background service is installed and registered with Windows.
Service Connection	Confirms that the client application can communicate with the background service.
Initial Profile Selection	Prompts the user to select a privacy profile (e.g., Recommended Settings) as the baseline configuration.
First Application	Applies the selected profile to establish the initial privacy configuration on the system.

Accessibility

Setup Mode is designed for users who may not have administrator rights. The background service handles all privileged operations, so the setup workflow does not require UAC elevation from the end user.

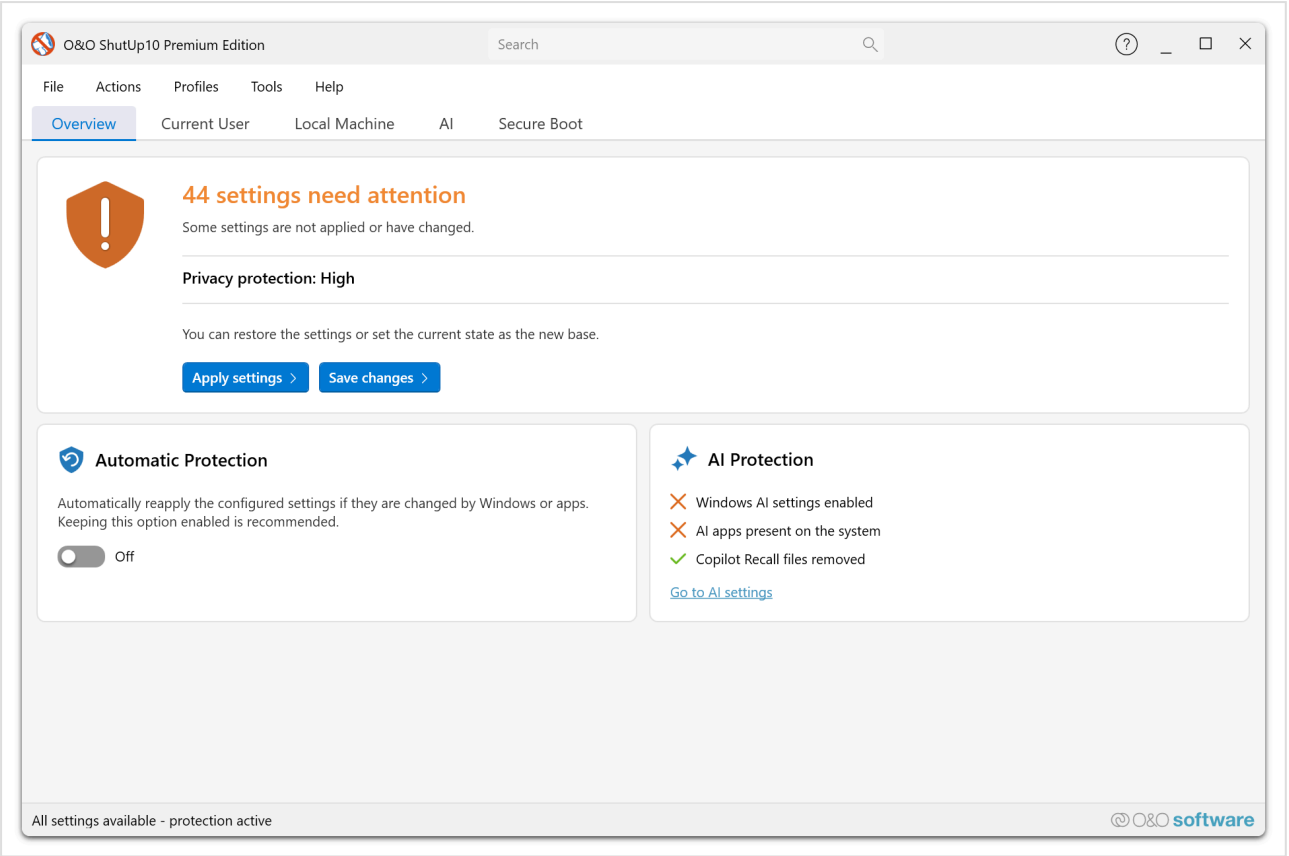
When Setup Mode Appears

- After a fresh installation of the Premium Edition.
- If the background service is uninstalled or unavailable.
- If the service connection is lost and cannot be re-established.

Once all setup steps are completed successfully, the Premium Overview automatically transitions to Overview Mode.

Overview Mode

Overview Mode provides a real-time dashboard of the current protection status and service health.



Once the Premium Edition is fully configured, the Premium Overview displays a summary view that gives users immediate visibility into the state of their privacy protection.

Dashboard Elements

Element	Description
Protection Status	Indicates whether automatic protection is currently active and enforcing the configured privacy settings.
Service Status	Shows whether the background service is running, stopped, or unavailable.
Active Profile	Displays the name of the currently applied privacy profile.
Last Enforcement	Timestamp of the most recent automatic re-application of privacy settings by the service.
Pending Changes	Number of settings that differ from the configured profile and are queued for re-application.

Usage Scenarios

- **Daily status check** — Open the application and immediately see whether protection is active and the service is healthy.
- **Post-update verification** — After a Windows update, verify that the service has automatically re-applied your privacy settings.
- **Troubleshooting** — If the service status shows as stopped or unavailable, the overview provides a starting point for diagnosing connectivity or service issues.

Accessibility

Overview Mode uses high-contrast status indicators and clear labels to ensure readability across all supported App View Modes, including High Contrast Black and High Contrast White themes. Status information is presented in a structured layout that is compatible with screen readers.

Relationship to Other Features

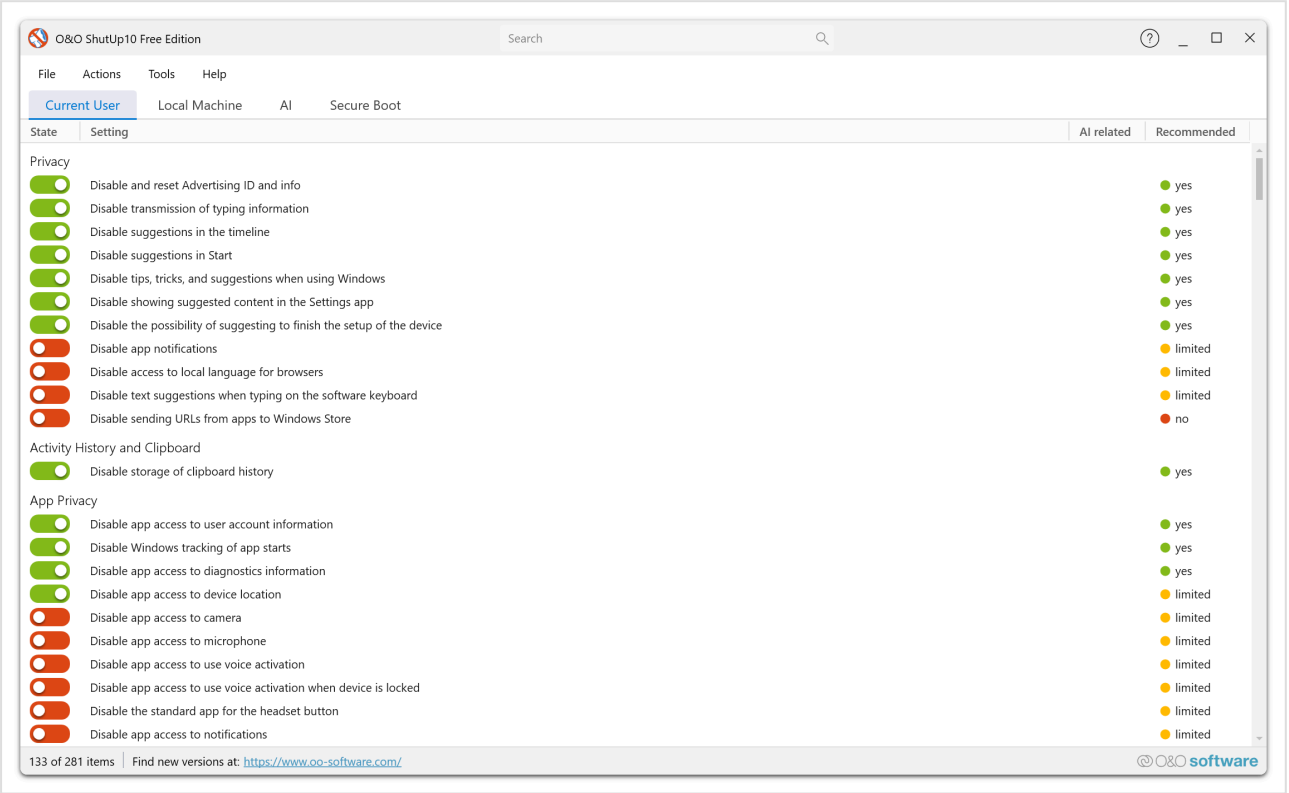
The Premium Overview integrates with several other Premium Edition features:

- **Automatic Protection** — The protection status and last enforcement time reflect the state of the Automatic Protection service.
- **Profiles Editor** — The active profile shown in Overview Mode corresponds to the profile managed through the Profiles Editor.
- **Settings Dialog** — Service-related configuration (notifications, hybrid mode, autostart) is managed through the Settings Dialog.

> **Tip**
>
> If the Premium Overview remains in Setup Mode after installation, verify that the O&O ShutUp10 service is installed and running. Check **Windows Services** (services.msc) or consult your IT administrator.

Privacy Settings

O&O ShutUp10 provides comprehensive control over almost 300 Windows privacy settings across more than 20 categories. This section covers all settings categories available in both the Free and Premium Editions.



Overview

Windows 10 and Windows 11 include numerous privacy-related settings spread across the Settings app, Group Policy, and the Windows Registry. O&O ShutUp10 consolidates these into a single interface, making it easy to review and adjust them. Settings are organized into clearly defined categories, each with individual recommendation levels.

Recommendation Levels

Each privacy setting includes a recommendation level:

Level	Description
Recommended	Safe for most users. No negative impact on core functionality.
Limited	Generally safe, but may affect certain personalization features.
Not recommended	May affect important functionality. Apply only with understanding of the impact.

> **Tip**
>
> Start by applying the **Recommended** settings. You can always adjust individual settings later.

Settings Categories

Privacy

Controls core Windows privacy behaviors including error reporting, notifications, and suggestions. These settings prevent Windows from transmitting personal information and displaying unsolicited content.

Key recommended settings:

- **Disable Windows Error Reporting** — Prevents crash reports (which may include memory dumps with personal data) from being uploaded to Microsoft.
- **Disable tips, tricks, and suggestions when using Windows** — Suppresses pop-ups in the Notification Pane and Info Center.
- **Disable showing suggested content in the Settings app** — Prevents promotional suggestions in system settings.
- **Disable suggestions in the timeline** — Blocks advertisements in the Windows Explorer timeline (e.g., OneDrive ads).
- **Disable app notifications** — Prevents apps from displaying notifications on tiles, lock screen, and desktop.

Telemetry and User Behavior

Manages the diagnostic and telemetry data that Windows sends to Microsoft for product improvement. Disabling these settings significantly reduces the amount of usage data, crash reports, and behavioral analytics transmitted from your device.

Key recommended settings:

- **Disable application telemetry** — Stops sending usage data and crash information to Microsoft.
- **Disable diagnostic data from customizing user experiences** — Prevents Microsoft from using your diagnostic data for personalization.
- **Disable diagnostic log collection** — Stops collection of detailed diagnostic logs.
- **Disable downloading of OneSettings configuration settings** — Prevents Microsoft from remotely configuring your device.

App Privacy

Controls which system resources and personal data Windows apps can access. This includes voice activation, camera, microphone, contacts, calendar, messaging, and more. Restricting app permissions limits what information third-party and built-in apps can collect.

Key recommended settings:

- **Disable app access to use voice activation** — Prevents apps from being activated by voice commands.
- **Disable app access to user account information** — Blocks apps from reading your account name and profile picture.
- **Disable app access to videos** — Prevents apps from accessing your video library.
- **Disable app access to use voice activation when device is locked** — Blocks voice-activated app access when the device is locked.

Cortana (Personal Assistant)

Controls Cortana and input personalization features. These settings prevent Microsoft from collecting voice, handwriting, and keyboard input data used to train Cortana and improve recognition.

Key recommended settings:

- **Disable Input Personalization** — Stops Microsoft from collecting voice, handwriting, and keyboard input data.
- **Disable the search highlights in the taskbar** — Removes visual search highlights that communicate with Microsoft servers.
- **Disable web search in Cortana** — Prevents search queries from being sent to Bing.

Location Services

Controls how Windows and apps use your physical location. Disabling location services prevents GPS, Wi-Fi, and sensor-based location tracking, which in turn stops location data from being sent to Microsoft and third-party apps.

Key recommended settings:

- **Disable app access to your location** — Prevents apps from accessing your physical location.
- **Disable sensors for locating the system and its orientation** — Deactivates GPS and gyroscope sensors (may affect screen rotation on tablets).
- **Disable functionality to locate the system** — Blocks system-level location tracking.
- **Disable scripting functionality to locate the system** — Prevents script-based location detection.

Search

Controls Windows Search behavior, including web search integration and search history collection.

Key recommended settings:

- **Disable web search in Start Menu** — Prevents Start menu search queries from being sent to Bing.

Synchronization of Windows Settings

Manages the synchronization of your Windows settings across devices using a Microsoft account. Settings, passwords, language preferences, and design choices are stored on Microsoft servers when synchronization is active.

Key recommended settings:

- **Disable synchronization of all settings** — Stops all Windows settings from being synced to Microsoft servers.
- **Disable synchronization of credentials (passwords)** — Prevents passwords from being stored and synced via Microsoft servers.
- **Disable synchronization of language settings** — Stops language preferences from being shared across devices.
- **Disable synchronization of design settings** — Prevents theme and visual settings from being synced.

Security

Controls security-related features that overlap with privacy, including Wi-Fi Sense, DRM, the steps recorder, and the Customer Experience Improvement Program. Adjusting these settings reduces the data shared with Microsoft while maintaining core security.

Key recommended settings:

- **Disable WiFi Sense** — Prevents automatic connection to contacts' Wi-Fi networks and sharing of your Wi-Fi password via Microsoft servers.
- **Disable user steps recorder** — Stops automatic recording of all actions on your computer (including screenshots and typed text).
- **Disable Internet access of Windows Media Digital Rights Management (DRM)** — Blocks DRM-related Internet communication (only if you do not use DRM-protected media).

- **Disable participation in Customer Experience Improvement Program** — Stops sending hardware and software usage data to Microsoft.

Windows Update

Controls how Windows downloads and installs updates, including peer-to-peer delivery, automatic driver updates, and optional/preview updates. While security updates are critical, some update features transmit data or install non-essential content.

Key recommended settings:

- **Disable Windows Update via peer-to-peer** — Stops your computer from sharing update data with other PCs over the Internet.
- **Disable optional updates (including preview updates)** — Prevents installation of unfinished preview updates.
- **Activate deferring of upgrades** — Delays feature upgrades so you can install them at a time of your choosing.

Microsoft Edge (new version based on Chromium)

Controls privacy and telemetry settings specific to the Chromium-based Microsoft Edge browser. These settings manage data collection, autofill behavior, cloud services, and promotional content within Edge.

Key recommended settings:

- **Disable automatic sign-in from web to browser** — Prevents automatic browser sign-in when signing into Microsoft websites.
- **Disable visual search** — Stops images from being sent to Bing for visual search.
- **Disable text prediction in forms** — Prevents cloud-based text prediction in browser form fields.
- **Disable cloud-based tab services** — Stops tab data from being synced to Microsoft cloud services.
- **Hide Microsoft Rewards** — Removes Microsoft Rewards promotional content from the browser.

Microsoft Edge (legacy version)

Controls privacy settings for the legacy (non-Chromium) version of Microsoft Edge. These settings manage form suggestions, search history, web tracking, and the Edge bar.

Key recommended settings:

- **Disable tracking in the web** — Enables Do Not Track signals in the legacy Edge browser.
- **Disable form suggestions** — Prevents Edge from remembering and suggesting form data.
- **Disable showing search history** — Stops Edge from displaying previous search queries.
- **Disable Edge bar** — Removes the Edge bar overlay from the desktop.

Microsoft Office

Controls privacy and telemetry settings for Microsoft Office applications. These settings manage connected experiences, diagnostic data, and feedback mechanisms that transmit usage information to Microsoft.

Key recommended settings:

- **Disable connected experiences with content analytics** — Stops Office from sending entered data to Microsoft's cloud for analysis.
- **Disable diagnostic data submission** — Prevents Office from transmitting diagnostic usage data.
- **Disable Microsoft Office surveys** — Blocks in-product survey prompts.
- **Disable participation in the Customer Experience Improvement Program** — Stops sending Office usage data to Microsoft.

Microsoft 365

Additional privacy settings specific to Microsoft 365 cloud-connected features and services.

Windows Explorer

Controls privacy-related behaviors in Windows Explorer, including OneDrive integration, Start menu suggestions, and recently opened items tracking.

Key recommended settings:

- **Disable ads in Windows Explorer/OneDrive** — Removes advertisements and sync provider notifications from Explorer.
- **Disable Microsoft OneDrive** — Fully disables Microsoft's cloud storage integration.
- **Disable OneDrive access to network before login** — Prevents OneDrive from synchronizing before users log in.
- **Disable occasionally showing app suggestions in Start menu** — Removes app advertisements from the Start menu.

Lock Screen

Controls the information displayed on the Windows lock screen, including notifications, advertisements, and Windows Spotlight content that communicate with Microsoft servers.

Key recommended settings:

- **Disable fun facts, tips, tricks, and more on your lock screen** — Removes advertisements and sponsored content from the lock screen.
- **Disable notifications on lock screen** — Prevents potentially private app notifications from being visible without logging in.
- **Disable Windows Spotlight** — Stops Microsoft from displaying curated images and content on the lock screen.

Taskbar

Manages privacy settings related to the Windows taskbar, including widgets, search box, news feed, and social features that exchange data with Microsoft servers.

Key recommended settings:

- **Disable widgets in Windows Explorer** — Prevents Windows 11 widgets from exchanging data with Microsoft servers.
- **Disable search box in task bar** — Removes the search box that sends queries to Microsoft.
- **Disable news and interests in the task bar** — Removes the news feed that transmits browsing and interest data.
- **Disable People icon in the taskbar** — Removes the People social feature from the taskbar.

Activity History and Clipboard

Controls the recording of user activities and clipboard history. Windows can track your activities across apps and devices, and store clipboard contents for cloud-based sharing.

Key recommended settings:

- **Disable the submission of user activities to Microsoft** — Stops activity data from being sent to Microsoft servers.
- **Disable storing users' activity history** — Prevents Windows from recording your application usage history.
- **Disable storage of clipboard history** — Stops Windows from retaining clipboard contents, reducing potential security risks.
- **Disable the transfer of the clipboard to other devices via the cloud** — Prevents clipboard data from being synced across devices through Microsoft servers.

Microsoft Defender and Microsoft SpyNet

Controls data sharing behaviors of Microsoft Defender, including sample submission and SpyNet membership. These settings manage what security-related data is sent to Microsoft for threat analysis.

Key recommended settings:

- **Disable submitting data samples to Microsoft** — Prevents Defender from sending file samples for cloud analysis.
- **Disable Microsoft SpyNet membership** — Stops participation in the Microsoft SpyNet telemetry network.
- **Disable reporting of malware infection information** — Prevents malware detection reports from being sent to Microsoft.

> **Caution**
>
> Do not disable Microsoft Defender itself unless you have an alternative, regularly updated antivirus solution in place.

Microsoft Copilot (in Windows)

Controls AI-related features in Windows, including the Microsoft Copilot assistant, the Copilot keyboard shortcut, and AI-powered features in built-in apps like Paint.

Key recommended settings:

- **Disable the Windows Copilot** — Fully disables the Copilot AI assistant in Windows.
- **Disable the Copilot button from the taskbar** — Removes the Copilot button from the taskbar.
- **Disable the Windows Copilot key on the keyboard** — Prevents the dedicated Copilot keyboard key from launching the assistant.
- **Disable the Image Creator in Microsoft Paint** — Disables AI-powered image generation in Paint.
- **Disable AI-powered image fill in Microsoft Paint** — Disables AI-powered fill features in Paint.

Mobile Devices

Controls the integration between your PC and mobile devices, including Phone Link and related notifications.

Key recommended settings:

- **Disable Phone Link app** — Disables the Phone Link application.
- **Disable connecting the PC to mobile devices** — Prevents PC-to-phone connectivity features.
- **Disable access to mobile devices** — Blocks mobile device access entirely.
- **Disable showing suggestions for using mobile devices with Windows** — Removes promotional notifications about mobile device features.

Miscellaneous

Covers additional privacy-related settings that do not fit into other categories, including feedback reminders, automatic app installations, and network connectivity checks.

Key recommended settings:

- **Disable feedback reminders** — Stops Microsoft from periodically requesting feedback and transferring diagnostic data.
- **Disable automatic installation of recommended Windows Store Apps** — Prevents Windows from silently installing promoted apps.
- **Disable tips, tricks, and suggestions while using Windows** — Suppresses promotional pop-ups and suggestions throughout the OS.

- **Disable Key Management Service Online Activation** — Blocks periodic activation verification checks with Microsoft (use only if you understand the implications).

Gaming

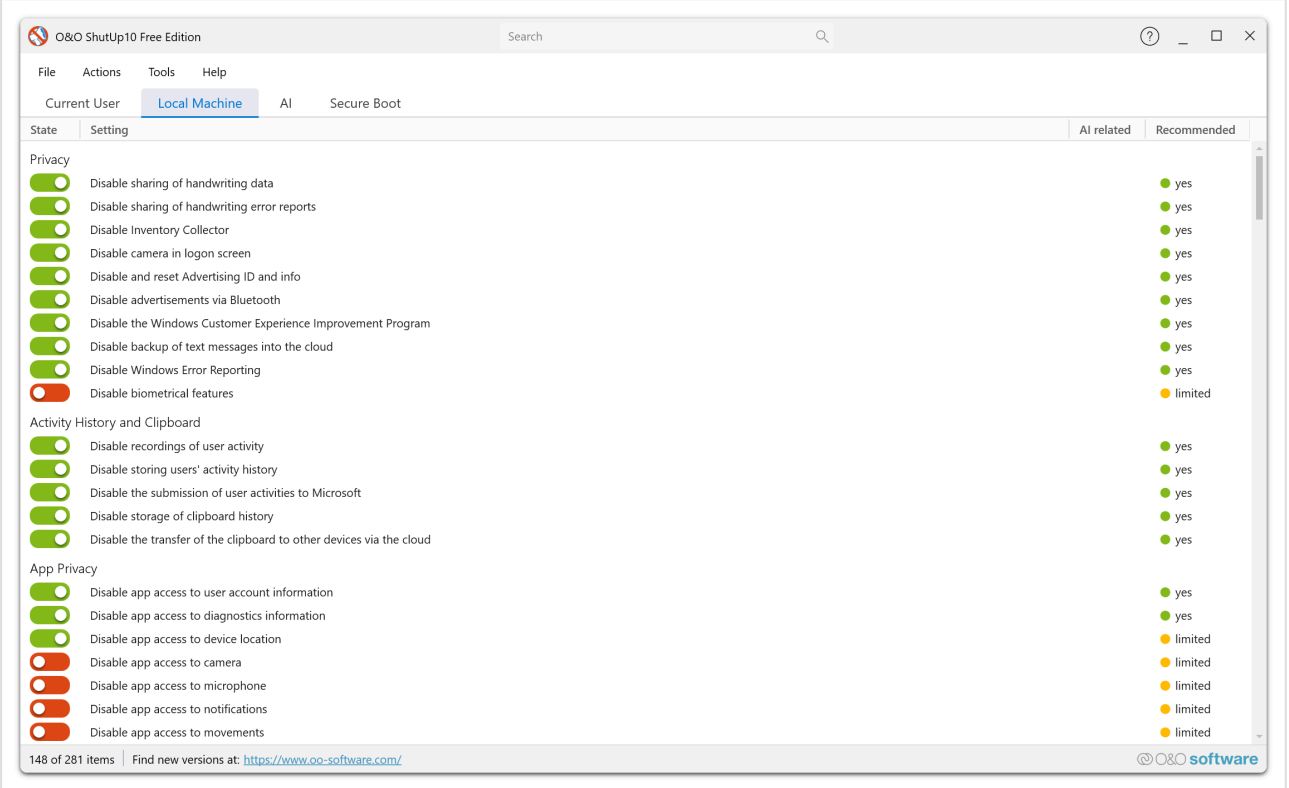
Controls gaming-related features that may collect data or cause unwanted behavior.

Key recommended settings:

- **Disable Xbox Game Bar and Game DVR** — Disables the Game Bar, Game DVR, and app capture functionality, preventing unwanted Microsoft Store prompts.

Telemetry Control

O&O ShutUp10 allows you to manage the telemetry and diagnostic data that Windows sends to Microsoft. These settings are available in both the Free and Premium Editions.



Overview

Windows collects diagnostic and usage data (telemetry) and sends it to Microsoft for product improvement and troubleshooting. The amount of data collected depends on the telemetry level configured on your system.

O&O ShutUp10 lets you control and reduce the telemetry data sent by Windows.

Key Telemetry Settings

Diagnostic Data Level

Windows offers multiple levels of diagnostic data collection. O&O ShutUp10 lets you set the level to the minimum required, reducing the amount of data shared with Microsoft.

Tailored Experiences

Microsoft uses diagnostic data to provide personalized tips, ads, and recommendations. You can disable tailored experiences to prevent your diagnostic data from being used for personalization.

Feedback Frequency

Windows periodically asks for feedback. You can control how often Windows prompts you for feedback, or disable feedback requests entirely.

Diagnostic Data Viewer

Windows includes a Diagnostic Data Viewer tool. O&O ShutUp10 can disable the collection pipeline that feeds this viewer if you prefer to minimize diagnostic data storage.

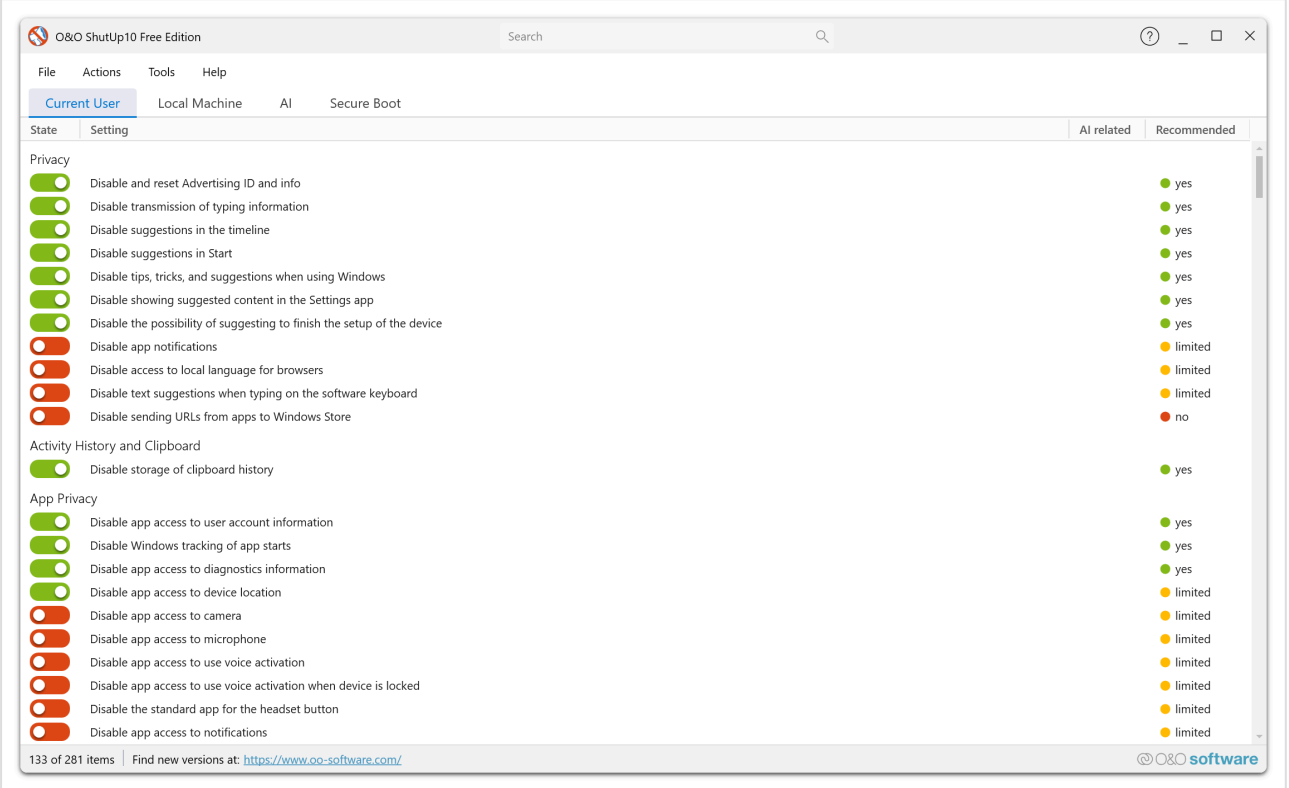
Error Reporting

Windows Error Reporting sends crash and error data to Microsoft. You can manage whether this information is collected and sent.

> **Note**
>
> Reducing telemetry to the lowest level may limit Microsoft's ability to identify and fix issues specific to your configuration, but significantly improves your privacy.

Location Services

O&O ShutUp10 gives you control over how Windows and its apps use your location data. These settings are available in both the Free and Premium Editions.



Overview

Windows uses location services to provide location-aware features such as weather, maps, and location-based reminders. While useful, these services also transmit your physical location to Microsoft and third-party apps.

What You Can Control

System-Wide Location Access

Disable location access for the entire system. When turned off, no apps or services can access your device's location.

Per-App Location Permissions

Control which individual apps are allowed to access your location data.

Location History

Windows stores a history of locations your device has been to. O&O ShutUp10 lets you disable location history collection.

Geofencing

Some apps use geofencing to trigger actions when you enter or leave a specific area. You can disable this functionality.

Location-Based Advertising

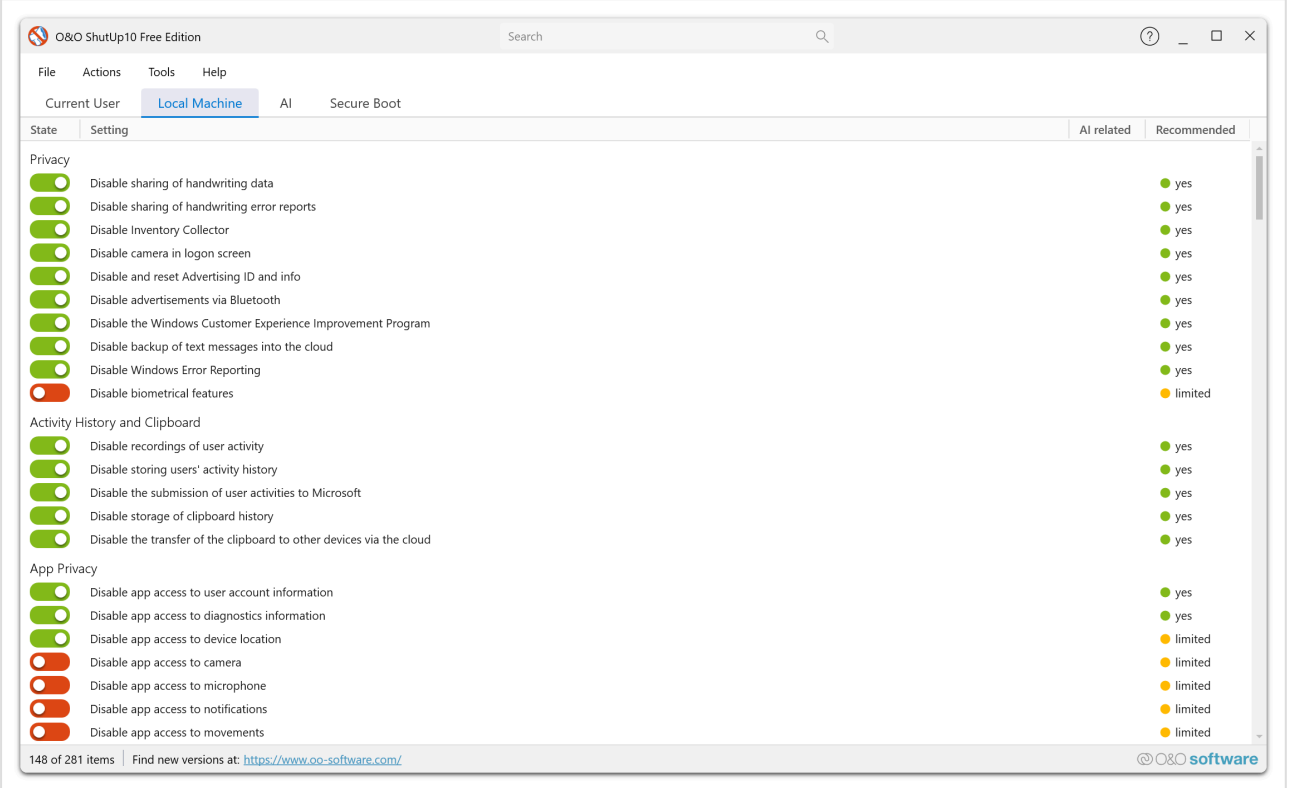
Advertising networks may use your location to serve targeted ads. You can prevent your location data from being used for advertising purposes.

Tip

If you do not use location-based apps (maps, weather widgets, etc.), disabling location services entirely is recommended for maximum privacy.

Windows Update Settings

O&O ShutUp10 provides control over Windows Update behavior. These settings are available in both the Free and Premium Editions.



Overview

Windows Update is essential for security and stability, but it also includes features that may affect your privacy, such as peer-to-peer update sharing and automatic driver downloads.

What You Can Control

Update Delivery Optimization

Windows can share downloaded updates with other PCs on your local network or over the internet (peer-to-peer delivery). O&O ShutUp10 lets you disable this feature or limit it to your local network only.

Automatic Driver Updates

Windows Update may automatically download and install drivers from Microsoft. You can control whether this happens or manage driver updates manually.

Automatic App Updates

The Microsoft Store automatically updates apps in the background. You can control this behavior through O&O ShutUp10.

Automatic Windows Updates

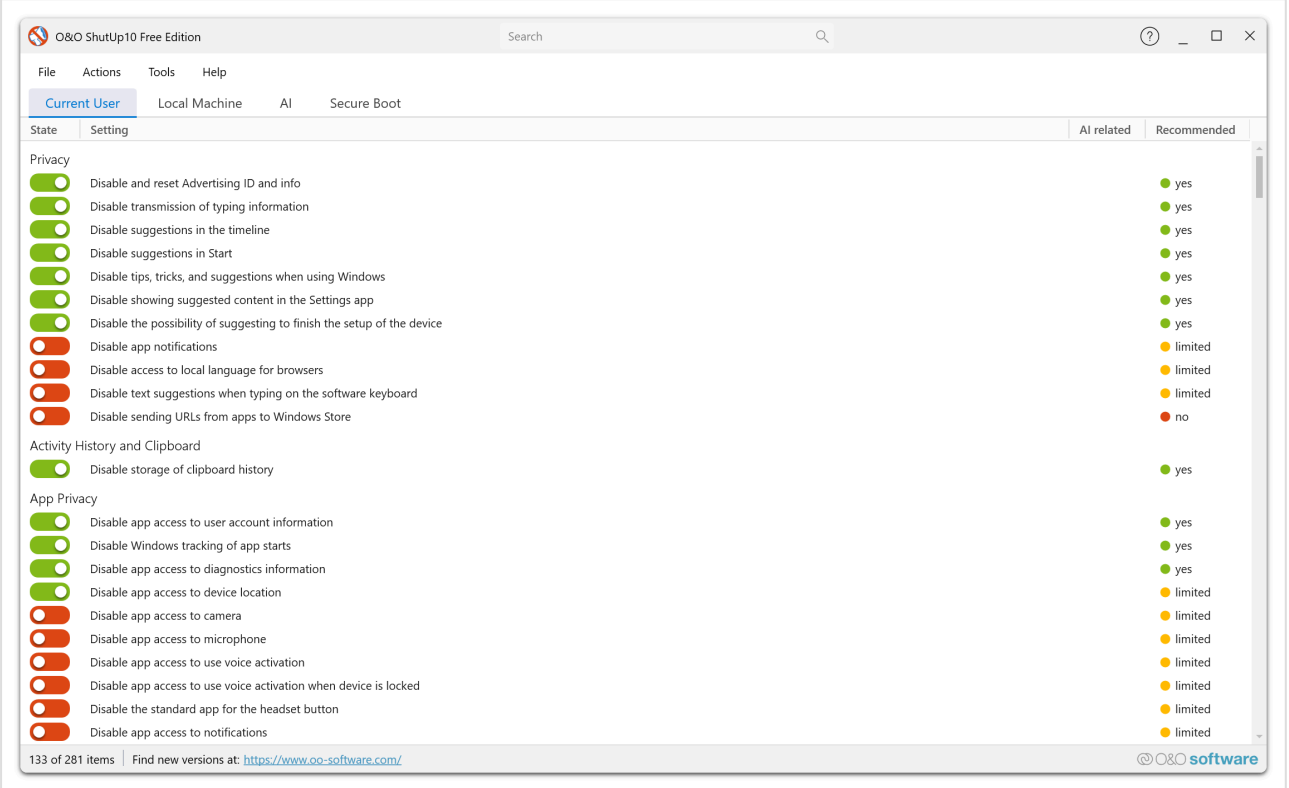
Control how Windows handles update downloads and installation schedules.

Caution

Disabling Windows Update features may leave your system without critical security patches. Only adjust these settings if you have an alternative update strategy in place.

Cortana & Search Settings

O&O ShutUp10 provides control over Cortana and Windows Search behavior. These settings are available in both the Free and Premium Editions.



Overview

Cortana and Windows Search can send search queries, voice data, and usage patterns to Microsoft. O&O ShutUp10 allows you to limit or disable these features for greater privacy.

What You Can Control

Web Search in Start Menu

By default, Windows sends your Start menu search queries to Bing. You can disable web search results to keep your searches local to your device.

Cortana Voice Activation

Cortana can listen for voice commands. You can disable voice activation to prevent any ambient audio processing.

Search History

Windows stores your search history to improve future results. You can disable search history collection.

Cloud Search

Windows Search can include results from your cloud services (OneDrive, Outlook, etc.). You can limit search to local content only.

Search Indexing

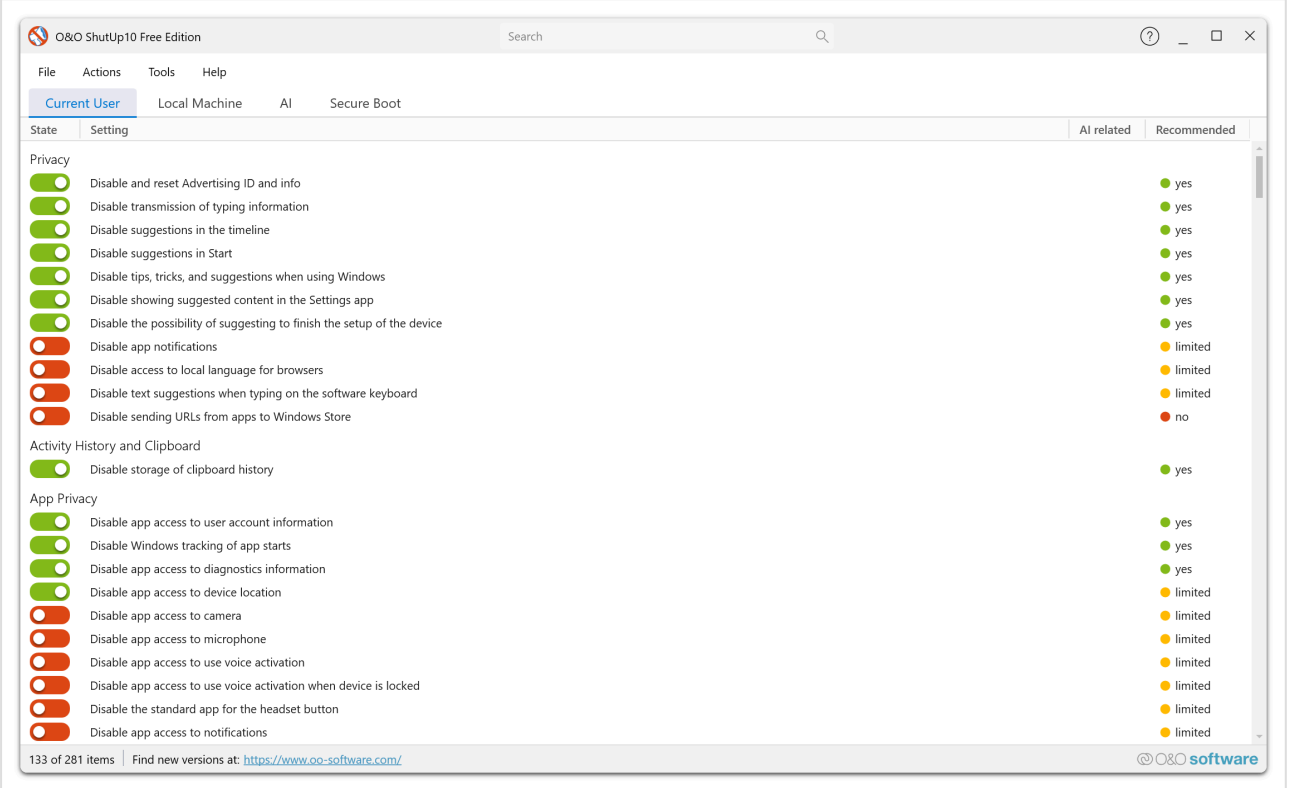
Control how Windows indexes files and content for search, including which locations are indexed and what content types are included.

Tip

Disabling web search in the Start menu is one of the most popular privacy adjustments, as it prevents every local search from being sent to Microsoft's servers.

App Permissions

O&O ShutUp10 lets you manage the permissions that Windows apps have access to. These settings are available in both the Free and Premium Editions.



Overview

Windows grants apps access to various system resources such as your camera, microphone, contacts, calendar, and more. O&O ShutUp10 lets you manage these permissions centrally rather than configuring each one individually through Windows Settings.

What You Can Control

Camera Access

Control which apps can access your device's camera. You can disable camera access system-wide or manage it per app.

Microphone Access

Control which apps can access your microphone. This is particularly important for privacy, as microphone access can be used for ambient listening.

Contacts Access

Manage which apps can read your contacts list.

Calendar Access

Control which apps can access your calendar entries.

Call History

Manage access to your call history, if applicable.

Email Access

Control which apps can access your email accounts and messages.

Messaging Access

Manage which apps can read or send text messages.

Notifications Access

Control which apps can access your notifications.

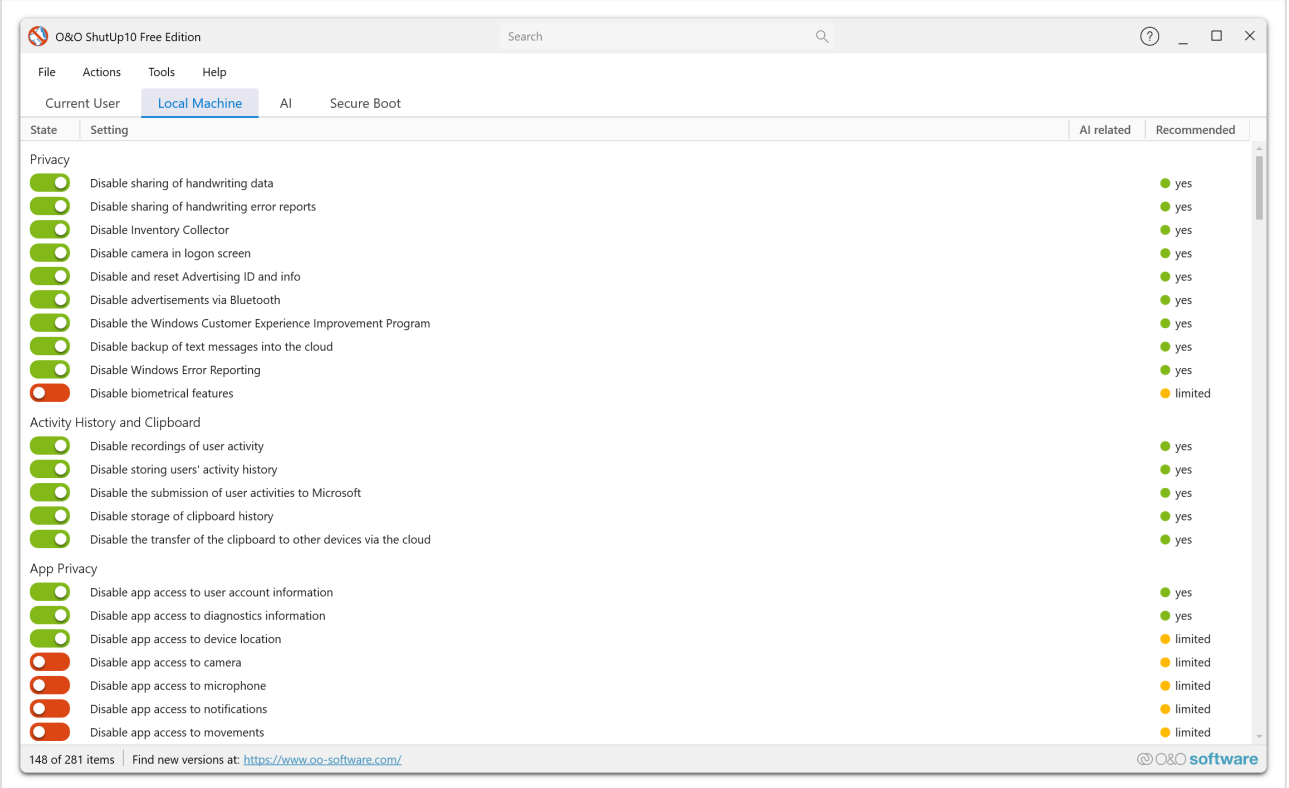
Account Information

Manage which apps can access your account name, picture, and other profile information.

> **Note**
>
> Restricting app permissions may cause some apps to lose functionality. Review each permission carefully before disabling it.

Windows Explorer & Advertising

O&O ShutUp10 provides control over Windows Explorer behavior and advertising-related settings. These settings are available in both the Free and Premium Editions.



Overview

Windows Explorer and the Windows shell include several features that display advertisements, suggestions, and promotional content. O&O ShutUp10 lets you disable these to create a cleaner, distraction-free experience.

What You Can Control

Sync Provider Notifications

Windows Explorer can display notifications from sync providers like OneDrive. You can disable these notifications.

Tips and Suggestions

Windows may show tips about Windows features and suggestions for apps. You can disable these prompts.

Start Menu Suggestions

The Start menu can display app suggestions (essentially advertisements for Microsoft Store apps). O&O ShutUp10 lets you disable these.

Lock Screen Ads

The Windows lock screen can display tips, tricks, and advertisements. You can configure the lock screen to show only your chosen background.

Timeline and Activity History

Windows Timeline tracks your activities across apps and devices. You can disable activity history collection and the Timeline feature.

OneDrive Integration

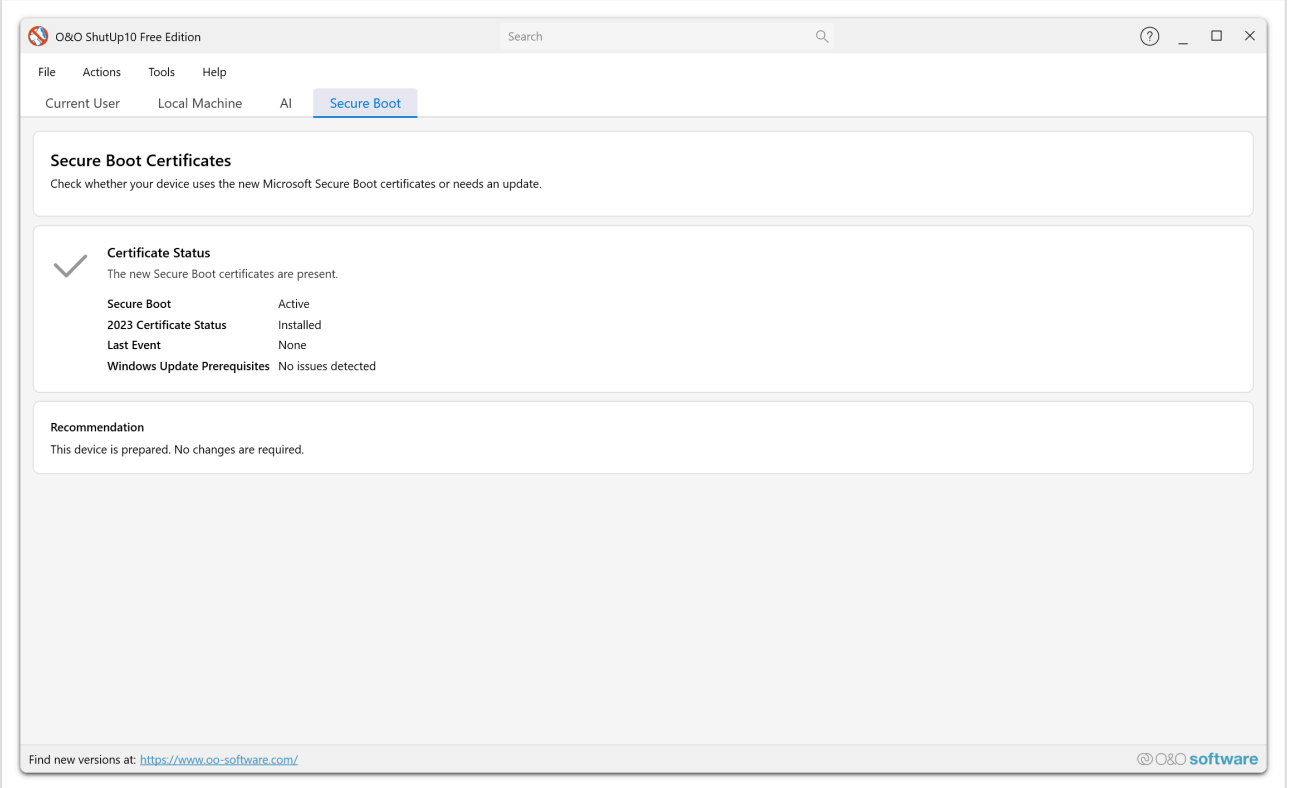
Control the level of OneDrive integration in Windows Explorer, including auto-start and promotional content.

Tip

Disabling advertising-related settings in Windows Explorer is recommended for all users and has no negative impact on functionality.

Security Settings

O&O ShutUp10 includes control over certain Windows security-related settings. These settings are available in both the Free and Premium Editions.



Overview

While O&O ShutUp10 is primarily a privacy tool, some Windows security features overlap with privacy. For example, cloud-based malware detection sends file information to Microsoft, and certain security features transmit telemetry data. O&O ShutUp10 lets you fine-tune these settings.

What You Can Control

Windows Defender Cloud Protection

Windows Defender can send file samples and detection information to Microsoft's cloud for enhanced protection. You can control this feature if you prefer to keep file information local.

Automatic Sample Submission

Windows Defender may automatically submit suspicious file samples to Microsoft for analysis. O&O ShutUp10 lets you disable this automatic submission.

Windows Security Notifications

Control the notifications displayed by Windows Security (formerly Windows Defender Security Center).

User Account Control (UAC)

Fine-tune UAC behavior, including notification levels and admin approval mode.

Caution

Adjusting security settings may reduce the effectiveness of Windows Defender or other security features. Only modify these settings if you have alternative security measures in place.

Frequently Asked Questions

This FAQ covers the most common questions about O&O ShutUp10, Windows privacy settings, and best practices for managing privacy on Windows 10 and Windows 11.

General Questions

What is O&O ShutUp10?

O&O ShutUp10 is a free antispy tool developed by O&O Software GmbH for Windows 10 and Windows 11. It provides a single, user-friendly interface to manage almost 300 privacy-related settings that are otherwise spread across the Windows Settings app, Group Policy, and the Windows Registry. The tool lets you decide which telemetry, tracking, and data-sharing features to disable — without requiring deep technical knowledge.

For a full overview, see the Introduction.

Is O&O ShutUp10 really free?

Yes. The **Free Edition** of O&O ShutUp10 is completely free of charge for personal and commercial use. It is a portable application — no installation is required. You simply download and run the executable.

O&O Software also offers a **Premium Edition** with additional features such as automatic background protection and a client/service architecture. The Premium Edition is a paid product aimed at professional and enterprise environments.

Does O&O ShutUp10 work on both Windows 10 and Windows 11?

Yes. O&O ShutUp10 supports both Windows 10 and Windows 11. The tool is regularly updated to cover new privacy-relevant settings introduced by Microsoft in both operating systems. Some settings are version-specific and will only appear when running on the applicable Windows version.

Is O&O ShutUp10 safe to use? Can it damage my system?

O&O ShutUp10 modifies Windows privacy settings through documented registry keys and group policy entries — the same mechanisms that Windows itself and system administrators use. It does not delete system files, modify boot configurations, or alter core operating system components.

Every change made by O&O ShutUp10 is fully reversible. The tool creates a system restore point before applying changes (if enabled), and you can undo any individual setting or restore all defaults from within the application.

> **Caution**
>
> Disabling certain settings (especially those marked **Not recommended**) can affect system functionality. Always review the recommendation level and description of each setting before applying it.

Installation and System Requirements

Does O&O ShutUp10 require installation?

The **Free Edition** does not require installation. It is a portable executable — download it, run it, and it works immediately. No files are left on your system after you close it (other than the privacy setting changes you applied).

The **Premium Edition** uses a client/service architecture and does require installation, as the background service needs to be registered with Windows to provide automatic, proactive protection.

Does O&O ShutUp10 require administrator privileges?

Yes. Because O&O ShutUp10 modifies system-level registry keys and group policy settings, it requires **administrator rights** to run. The Free Edition will prompt for elevation (UAC) each time you start it. The Premium Edition's background service runs with the necessary privileges automatically, so end users do not need administrator access on their machines.

Using O&O ShutUp10

What do the colored toggle switches mean?

O&O ShutUp10 uses a traffic-light color scheme for its toggle switches:

Color	Meaning
Green (on)	The privacy protection is **active** — the corresponding Windows feature is disabled.
Red (off)	The privacy protection is **inactive** — the Windows feature is running with its default behavior.

A **green** toggle means the tool has blocked that particular tracking or data-sharing feature, while a **red** toggle means Windows is operating normally for that setting.

What are the recommendation levels and which settings should I apply?

Each setting in O&O ShutUp10 includes a recommendation level:

Level	Description
Recommended	Safe for most users. Disabling these features has no negative impact on core Windows functionality.
Limited	Generally safe, but may affect certain personalization or convenience features (e.g., Cortana, activity history).
Not recommended	May affect important functionality such as Windows Update delivery, Windows Defender, or system activation. Only apply these if you fully understand the consequences.

> **Tip**
>
> If you are unsure where to start, apply only the **Recommended** settings first. You can review and adjust individual settings at any time.

For a full description of settings categories, see the Privacy Settings Overview.

Can I apply all recommended settings at once?

Yes. O&O ShutUp10 provides an **Actions** menu that lets you apply all settings of a given recommendation level in one step. You can choose to apply all **Recommended** settings, all **Recommended and Limited** settings, or all settings regardless of level. This is the fastest way to configure your system.

What are profiles, and how do I use them?

Profiles allow you to save your current configuration (the state of all toggle switches) to a file and reload it later. This is useful for:

- **Backing up** your preferred settings before making changes.
- **Sharing** a consistent configuration across multiple computers.
- **Restoring** your preferred state after a Windows update resets your privacy settings.

You can export a profile via **File → Export Settings** and import it with **File → Import Settings**. Profile files use the `.cfg` file format.

For more details, see the Profiles & Export documentation.

Recommendation Levels and Profiles

What is the difference between "Recommended," "Limited," and "Not recommended" settings?

These levels indicate the potential impact of disabling a Windows feature:

- **Recommended** settings disable telemetry and tracking features that most users do not need. Applying these settings improves your privacy with no noticeable impact on everyday use.
- **Limited** settings disable features that some users may rely on, such as Cortana, web search integration, or activity history synchronization. Disabling them is safe but may change your workflow.
- **Not recommended** settings control features that are important for system stability or security, such as Windows Update peer-to-peer delivery, Windows Defender telemetry, or system activation. Disable these only if you have a specific reason and understand the potential side effects.

Will applying "Not recommended" settings break my computer?

Applying "Not recommended" settings will not permanently damage your computer, but it can cause undesired behavior. Examples include:

- **Windows Update issues** — Disabling update delivery optimization may slow down or prevent updates from downloading.
- **Reduced security** — Disabling Defender sample submission or SpyNet membership reduces the effectiveness of real-time threat detection.
- **Activation problems** — Disabling KMS Online Activation can cause Windows activation to fail on volume-licensed systems.

All changes are reversible. If you notice problems after applying a setting, simply toggle it back to its original state or use the **Undo** feature.

Undoing Changes and Restoring Defaults

How do I undo changes made by O&O ShutUp10?

There are several ways to revert changes:

1. **Toggle individual settings** — Click any green toggle to turn it red (off), restoring the Windows default for that setting.
2. **Undo all changes** — Use the **Actions** menu and select **Undo all changes** to reset every setting to its Windows default.
3. **Import a saved profile** — If you exported your settings before making changes, import the saved profile to restore your previous configuration.
4. **System Restore** — If you created a system restore point before applying changes (O&O ShutUp10 can prompt you to do this), you can use Windows System Restore to roll back your entire system to the earlier state.

Does O&O ShutUp10 create a system restore point automatically?

O&O ShutUp10 offers to create a system restore point before applying changes. When you first apply settings, the tool will prompt you to create one. It is strongly recommended to accept this prompt, as it provides a safety net that lets you roll back all changes via the standard Windows System Restore feature.

Windows Updates and Compatibility

Will Windows Update reset my privacy settings?

Yes, this is a known and common issue. Major Windows feature updates (e.g., upgrading from Windows 10 22H2 to Windows 11 23H2, or applying annual feature updates) can reset some or all of the privacy settings you changed. Microsoft's update process may restore default telemetry and tracking configurations.

What to do after a major update:

1. Run O&O ShutUp10 again and review your settings — any reset toggles will appear red.
2. Re-apply your preferred settings manually, or import a previously saved profile.
3. The **Premium Edition** handles this automatically: its background service detects when settings have been reverted and re-applies your preferred configuration without manual intervention.

Is it safe to use O&O ShutUp10 alongside Windows Update?

Yes. O&O ShutUp10 does not interfere with the Windows Update mechanism itself. Security updates, cumulative updates, and driver updates will continue to download and install normally.

However, if you disable specific update-related settings (such as **peer-to-peer update delivery** or **optional/preview updates**), those particular behaviors will change as intended. Critical security updates are not affected by any of the recommended settings.

Windows Defender and Security

Does O&O ShutUp10 disable Windows Defender?

O&O ShutUp10 does **not** disable Windows Defender by default. The Defender-related settings in the tool control **data-sharing behaviors** — such as whether Defender sends file samples to Microsoft for cloud analysis or participates in the Microsoft SpyNet telemetry network.

Disabling these data-sharing features reduces the information sent to Microsoft but may slightly reduce the effectiveness of Defender's cloud-based threat detection. The core antivirus engine, real-time protection, and local signature-based scanning remain fully functional.

> **Caution**
>
> Do not disable Windows Defender entirely unless you have an alternative, regularly updated antivirus solution installed and active.

Can I use O&O ShutUp10 together with third-party antivirus software?

Yes. O&O ShutUp10 manages privacy settings at the operating system level and does not conflict with third-party antivirus software. If you are already using a third-party solution (which typically disables Windows Defender automatically), you can safely apply all Defender-related privacy settings in O&O ShutUp10 without concern.

Windows Privacy Settings

What is Windows telemetry, and why should I care?

Windows telemetry refers to the diagnostic and usage data that Windows collects and sends to Microsoft. This data can include:

- **Hardware and software inventory** — Details about your device, installed applications, and drivers.
- **Usage patterns** — How you use Windows features, apps, and services.
- **Crash reports and error logs** — Information about application and system failures, which may include memory dumps containing personal data.
- **Browsing and search data** — Queries typed into the Start menu, Cortana, or Edge.

Microsoft uses this data for product improvement and personalization, but many users and organizations prefer to minimize or eliminate this data collection for privacy, compliance, or security reasons.

O&O ShutUp10 lets you control telemetry at a granular level. Applying the **Recommended** telemetry settings significantly reduces data collection without affecting system functionality.

For details on telemetry settings, see the Telemetry Control documentation.

What is the difference between Windows 10 and Windows 11 privacy settings?

Windows 11 introduced several new privacy-relevant features and expanded existing ones:

- **Widgets and News Feed** — Windows 11 added a widgets panel that communicates with Microsoft servers. O&O ShutUp10 includes settings to disable this.
- **Microsoft Copilot** — Windows 11 introduced an AI assistant (Copilot) with its own data collection. O&O ShutUp10 provides settings to disable Copilot and its keyboard shortcut.
- **Enhanced telemetry** — Windows 11 expanded certain telemetry categories. O&O ShutUp10 covers these additional data points.
- **Snap Layouts and Desktop organization** — Some new UI features have telemetry components that can be controlled.
- **Phone Link integration** — Deeper mobile device integration in Windows 11 introduces additional privacy considerations.

O&O ShutUp10 automatically detects your Windows version and displays only the settings relevant to your system. Settings that apply only to Windows 11 will not appear on a Windows 10 machine, and vice versa.

What happens if I disable location services?

Disabling location services prevents Windows and apps from accessing your physical location via GPS, Wi-Fi positioning, or device sensors. This means:

- **Weather apps** will not automatically detect your location (you can still set a location manually).
- **Maps and navigation** will not be able to determine your position.
- **Find My Device** will not function.
- **Location-based reminders** (e.g., in Cortana) will not work.
- **Screen auto-rotation** on tablets may be affected if sensor access is also disabled.

For most desktop users, disabling location services has no practical downside. Tablet and laptop users who rely on GPS or location-based features should consider keeping this setting enabled.

See the Location Services documentation for details on individual location settings.

Should I disable Cortana and web search in the Start menu?

Disabling Cortana and web search prevents search queries typed into the Start menu from being sent to Microsoft's Bing servers. Instead, searches will only return local results (installed apps, files, and settings).

This is one of the most commonly applied privacy settings and is classified as **Recommended** in O&O ShutUp10. Most users find that local-only search is faster and more relevant to their needs, and it completely eliminates the transmission of search queries to Microsoft.

See the Cortana & Search documentation for all related settings.

Troubleshooting

A setting keeps reverting to its original state. What can I do?

Some Windows settings may be reset by:

- **Windows Update** — Feature updates and sometimes cumulative updates can restore default privacy settings.
- **Group Policy** — In domain-joined (enterprise) environments, group policy may override local settings.
- **Scheduled tasks** — Certain Windows scheduled tasks may periodically re-enable telemetry features.

Solutions:

1. Re-run O&O ShutUp10 after each major Windows update and re-apply your settings.
2. Export your settings as a profile so you can quickly re-import them.
3. Consider the **Premium Edition**, which automatically detects and re-applies settings that have been reverted.

O&O ShutUp10 shows a setting as "not available" or grayed out. Why?

A setting may be unavailable for several reasons:

- **Windows version mismatch** — The setting applies only to a Windows version you are not running (e.g., a Windows 11–only setting on a Windows 10 machine).
- **Edition limitation** — Some settings only apply to specific Windows editions (e.g., Pro, Enterprise, or Education) because they rely on Group Policy features not available in Home editions.
- **Feature not installed** — The Windows feature that the setting controls is not installed on your system (e.g., Microsoft Office settings when Office is not installed).

This behavior is expected and does not indicate a problem with O&O ShutUp10.

I applied settings and now something on my system is not working correctly. What should I do?

1. **Identify the affected functionality** — Determine what stopped working (e.g., Start menu search, a specific app, Windows Update).
2. **Open O&O ShutUp10** and look for settings related to the affected feature. The settings are organized by category (Search, Windows Update, Security, etc.).
3. **Toggle the suspected setting back** (from green to red) to restore the Windows default for that feature.
4. **Test** whether the issue is resolved.
5. If you are unable to identify the specific setting, use **Actions → Undo all changes** to restore all Windows defaults, then re-apply settings one category at a time to isolate the cause.
6. As a last resort, use **Windows System Restore** to revert to a restore point created before you applied the changes.

Enterprise and Advanced Use Cases

Can I use O&O ShutUp10 in a corporate or enterprise environment?

Yes. The **Premium Edition** is specifically designed for enterprise use. It features:

- **Client/service architecture** — A background service applies and maintains privacy settings without requiring end-user interaction or administrator rights.
- **Automatic re-application** — The service detects when Windows updates or group policy changes revert settings and re-applies your preferred configuration.
- **Centralized configuration** — Administrators can define a standard privacy profile and deploy it across multiple endpoints.

The **Free Edition** can also be used in enterprise environments, but it requires manual execution with administrator rights on each machine, making it less practical for large-scale deployments.

Can I deploy O&O ShutUp10 settings via command line or script?

Yes. O&O ShutUp10 supports command-line operation, which enables integration with deployment scripts, login scripts, or management tools. You can apply a saved profile (`.cfg` file) silently from the command line, making it suitable for automated deployment across multiple machines.

How does O&O ShutUp10 interact with Group Policy settings?

O&O ShutUp10 applies settings through the Windows Registry, which is the same mechanism used by Group Policy. In general:

- If a setting is managed by **local Group Policy**, O&O ShutUp10 can override it (since both write to the same registry locations).
- If a setting is enforced by **domain Group Policy** (in an Active Directory environment), the domain policy will take precedence and may override changes made by O&O ShutUp10.

> **Info**
>
> In enterprise environments, it is recommended to coordinate O&O ShutUp10 configurations with your Group Policy strategy to avoid conflicts.

Is O&O ShutUp10 compliant with GDPR and other data protection regulations?

O&O ShutUp10 itself does not collect, store, or transmit any user data. It is a local tool that modifies Windows settings on the device where it runs.

By using O&O ShutUp10 to disable telemetry, tracking, and data-sharing features in Windows, organizations can reduce the volume of personal data transmitted to Microsoft — which can support compliance with the **General Data Protection Regulation (GDPR)**, **CCPA**, and other data protection frameworks. However, O&O ShutUp10 is one component of a broader compliance strategy; organizations should consult their data protection officers and legal teams for comprehensive compliance guidance.

Where can I get help if my question is not answered here?

- **O&O Software Support:** https://www.oo-software.com/en/support
- **O&O Software Product Page:** https://www.oo-software.com/en/shutup10
- **Microsoft Privacy Documentation:** https://privacy.microsoft.com
- **Microsoft Windows Privacy Settings Reference:** https://support.microsoft.com/en-us/windows/windows-privacy-settings

For Premium Edition customers, priority support is available through the O&O Software support portal.