



Blanco Autopilot Detection & Touchless Recheck

Detect, re-verify, and certify - without reprocessing.

Evolving OS Security Creates Risk - Blanco Eliminates It

As operating systems evolve, ITADs face a growing challenge: once a device reconnects to the internet, could corporate data be restored?

Blanco Autopilot Detection eliminates that risk by automatically identifying Microsoft Autopilot, Intune, and other UEM enrollments during erasure-ensuring devices are fully unenrolled before resale or redeployment.

Now enhanced with Touchless Recheck, users can remotely confirm post-erasure enrollment status directly in the Blanco Management Portal (BMP). No reconnects, no reboots-just fast, automated verification that strengthens compliance and delivers audit-ready proof at scale.

Key Features & Benefits

Autopilot Detection

- ▶ Automatically identifies devices enrolled in Microsoft Autopilot during erasure.
- ▶ Detects enrollment directly within Blanco Drive Eraser (BDE), no separate WinPE client required.
- ▶ Provides instant visibility of enrolled assets within the Blanco Management Portal (BMP).
- ▶ Prevents the resale or redeployment of Autopilot-locked devices.
- ▶ Delivers certified, tamper-proof reporting for audit and compliance.

Touchless Recheck (New)

- ▶ Re-verifies Autopilot enrollment after customer unenrollment, without touching the device again.
- ▶ Performs bulk rechecks (up to 500 devices) directly through BMP.
- ▶ Updates reports with new enrollment status and timestamp for verified audit accuracy.
- ▶ Automatically re-signs reports to maintain compliance integrity.

Both Integrated into Processor Pro and Pro-Scale bundles via the common license pool.

WHY BLANCCO

Blanco Technology Group, a carbonneutral supplier, provides organizations with secure, compliant, and automated solutions that accelerate the transition to the circular economy.

All erasures are verified and certified through a tamper-proof audit trail. With nearly 25 years of responding to customer needs and 35+ patented or patent-pending ideas, Blanco is the industry standard in data erasure and mobile lifecycle solutions. Our dedication to technological innovation empowers top-tier enterprises, IT asset disposition (ITAD) vendors, and mobile industry stakeholders to protect end-of-life data against unauthorized access, comply with data protection requirements, extend the useable life of IT assets, accelerate operations, and enhance the mobile customer experience.

[View Our Certifications](#)

Find out how we can help

[Contact Us](#)



Summary

Blancco Autopilot Detection + Touchless Re-Check provides the industry's first end-to-end Autopilot verification workflows, automating both initial detection and post-erasure re-validation. By combining security, automation, and compliance, it empowers ITADs and enterprises to process assets faster, eliminate manual errors, and provide certified assurance that every device is ready for resale or redeployment.

Technical Specifications

MACHINE PROCESSING, HARDWARE DETECTION

Machine Processing

- ▶ Runs on any **Blancco Drive Eraser-supported machine** (x86 or x64 architecture).
- ▶ Compatible with both **online and offline** erasure workflows; internet connection recommended for Touchless Recheck.
- ▶ **Single-boot automation** - Autopilot Detection runs automatically within the erasure process, no extra imaging or manual steps.
- ▶ Processing speed identical to standard Drive Eraser runs - **no additional cycle time** added.

Hardware Detection

- ▶ Automatically detects **Autopilot, Intune, and UEM enrolment** through firmware, BIOS, and network identifiers.
- ▶ Supports **UEFI-based and legacy BIOS** systems across OEMs (HP, Dell, Lenovo, etc.).
- ▶ Identifies hardware attributes (CPU, RAM, storage, motherboard serials) for audit logging.
- ▶ Fully compatible with **Windows-based assets** and verified through **Blancco Management Portal (BMP)** reporting.

USABILITY, DEPLOYMENT & LANGUAGES

Blancco Autopilot Detection

- ▶ **Simple Deployment:** Built into Blancco Drive Eraser- no separate installation or setup needed.
- ▶ **Single-Boot Workflow:** Automatically detects Autopilot and UEM profiles during erasure.
- ▶ **Global Accessibility:** Managed through Blancco Management Portal and available in multiple interface languages.

Blancco Touchless Recheck

- ▶ Works only on devices that have an existing Drive Eraser report showing Autopilot status.
- ▶ Re-Check currently supports Windows Autopilot only.
- ▶ Requires stable connectivity between BMP and Microsoft Autopilot/Intune services.
- ▶ Bulk Re-Check limited to 500 devices per batch.

MINIMUM SYSTEM REQUIREMENTS

Blancco Autopilot Detection Infrastructure

- ▶ Requires at least one **Blancco Drive Eraser (BDE)** machine with **internet connectivity**.
- ▶ **No WinBuilder or WinPE image creation needed** - Autopilot Detection runs natively within Drive Eraser.
- ▶ Operates as a **single-boot workflow**, performing detection and erasure in one seamless session.
- ▶ Optional connection to the **Blancco Management Portal (BMP)** for centralized reporting and cloud-based rechecks.

Tools

- ▶ **Blancco Drive Eraser v6.17 or later** (supports Autopilot Detection natively).
- ▶ **Blancco Management Portal (BMP)** – provides visibility, reporting, and access to Touchless Recheck.
- ▶ **Touchless Recheck module** - enables post-erasure verification of Autopilot/UEM status directly via the cloud, without reconnecting the device.
- ▶ **Common License Pool** usage-based activation; Autopilot Detection and Touchless Recheck draw from the same pool (included in Scale and Pro-Scale bundles).

Blancco Touchless Recheck

- ▶ Blancco Management Portal (BMP) v3.3.0 or later.
- ▶ Blancco Drive Eraser (BDE) with Autopilot Detection enabled.
- ▶ Common License Pool Access: PID 80 (Detection) and PID 83 (Re-Check).
- ▶ Active internet connection to validate enrolment status via Microsoft APIs.

AUDITING & REPORTING

Blancco Autopilot Detection

- ▶ Autopilot status automatically logged in Blancco Drive Eraser report
- ▶ Show the Autopilot status to the operator using IBR Workflows popups

Blancco Touchless Recheck

- ▶ Centralized Visibility: All recheck events logged in the Blancco Management Portal(BMP) with full audit history.
- ▶ Timestamped Proof: Each verification includes date, device ID, and enrollment statusfor compliance validation.
- ▶ Integrated Reports: Detection and recheck results combined in one certified Blancco audit report.