



Blanco Removable Media Eraser

Secure Data Erasure for Removable Media Devices

Why Blanco

Blanco is the industry standard in data erasure and mobile device diagnostics. Blanco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail.

Blanco data erasure solutions have been tested, certified, approved and recommended by 18 governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

[View Our Certifications](#)

Blanco Removable Media Eraser protects against loss or theft of data from removable media supported by Microsoft Windows.

With Blanco Removable Media Eraser, you can permanently erase data using regulatory standards from removable media, including USB drives, SD memory cards, micro drives, CompactFlash cards, MP3 players and other flash memory storage devices in order to prove 100% compliance. Delivered to multiple users as a simple desktop application or MSI package, you can reduce the risk of data loss and fraud using security best practices through single data erasure or simultaneous erasure processes.

Key Benefits

Securely Erase Data in Live Environments, Flash Drives and Other Removable Media

- Permanently wipe multiple flash drives, rapidly and simultaneously
- Create on-demand, centralized data erasure stations within your organization

Flexible User Management for Process Efficiency and Reduced Costs

- Distribute among multiple users through a simple desktop application or MSI package
- Enhance process management by simultaneously erasing multiple devices and display the status of all connected units
- Save post-erasure report locally or integrate with Blanco Management Console

Fully Compliant and Tamper-Proof Reporting

- Automatically generate customized post-erasure reports, detail essential hardware information for a tamper-proof audit trail.
- Strengthen knowledge and awareness of internal policies and processes across the business with scheduling and integrated erasure routines.
- Stay compliant with industry standards and regulations, including PCI DSS, HIPAA, SOX, ISO 27001, ISO 27040 and EU General Data Protection Regulation.

Technical Specifications

ERASURE		USER MANAGEMENT	
<ul style="list-style-type: none"> Erases any type of flash-based removable storage media supported by Microsoft Windows Optional automatic formatting after erasure (NTFS) Supports all well known erasure algorithms including: <ul style="list-style-type: none"> Army Regulation, AR380-19 U.S. Department of Defense, 5220.22-M, Navy Staff Office Publication, NAVSO P-5239-26 Classification level SECRET or CONFIDENTIAL, Navy Staff Office Publication, NAVSO P-5239-26. Classification level TOP SECRET NIST Special Publication 800.88 Revision 1. Guidelines for Media Sanitization Conforms to recognized international erasure standards Optimized erasure speed 		<ul style="list-style-type: none"> Easy to install and extremely user-friendly MSI package can distribute to several users in a large organization Capable of simultaneously erasing multiple devices Displays the status of all connected units during erasure enhances process management 	
SUPPORTED MEDIA TYPES		REPORTING	
<ul style="list-style-type: none"> SB flash drive SmartMedia SecureDigital (SD/SDHC/miniSD) MultiMediaCard (MMC/MMCMobile/RS-MMC) Compact Flash (CF) Memory Stick Digital cameras with flash drives MP3 players with flash drives Other flash-based storage media 		<ul style="list-style-type: none"> Automatically generates a detailed erasure report after each erasure Report details include serial numbers and other hardware specifics Add custom fields in the report process to capture vital process information 	
SYSTEM REQUIREMENTS	AUDITING	LANGUAGE SUPPORT	
<ul style="list-style-type: none"> Windows 7 / Windows 8.1 and 8 / Windows 10 At least 200 MB of free disk space Mouse or keyboard 	<ul style="list-style-type: none"> Full auditing capabilities Standard XML report format for integration with Blancco Management Console 	<ul style="list-style-type: none"> English, French, German and Japanese <p>Please ask your Blancco sales representative for details.</p>	