



# Blancco Network Device Eraser

Secure Data Erasure for Network Switches and Routers

## Why Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco 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.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ 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](#)

Using patent-pending technology, Blancco Network Device Eraser permanently removes sensitive information from network routers switches and routers.

Now, ITADs can remove network configurations, IP addresses, cached files, user credentials, user data and more—accelerating what was once a heavily manual and device-specific factory reset process.

## Key Benefits

### Unmatched Efficiency and Security

- Dramatically increase throughput while decreasing labor costs
- Permanently sanitize Cisco switches and routers to NIST Clear (leaving device operating systems intact) or NIST Purge and NIST Purge - Full Overwrite (for complete erasure, including of the operating system)
- Ensure consistent erasure processes across Cisco device models
- Bypass passwords automatically for Cisco devices that do not use default passwords
- Directly reload the Operating System after an Erasure saving valuable time
- Erase multiple Cisco devices simultaneously and automatically, validating the erasure and providing a Certificate of Erasure

### Maximized Compliance and Reporting

- Ensure compliance with data protection regulations (including PCI DSS, HIPAA, SOX, ISO 27001, ISO 27040 and GDPR) and internal security or data management policies that identify controlled data
- Generate post-erasure reports—including detailed hardware information—for a tamper-proof audit trail

## Technical Specifications

| ERASURE   | USER MANAGEMENT  |  |
|---|--|--|
| <ul style="list-style-type: none"> <li>Erases to NIST Clear and NIST Purge levels               <ul style="list-style-type: none"> <li>NIST Clear leaves devices available for reuse</li> <li>NIST Purge ensures complete data removal before destruction, recycling or operating system reinstall</li> <li>NIST Purge - Full Overwrite adds an additional level of security by overwriting the entire file system</li> </ul> </li> <li>Provides automated password bypass</li> <li>Can erase multiple devices simultaneously</li> <li>Supports hot plugging devices</li> </ul> | <ul style="list-style-type: none"> <li>Portable—no installation required</li> <li>Graphical user interface (GUI) and command line versions available</li> <li>Displays the status to all connected units during erasure to enhance process management</li> </ul>   |  |
| SUPPORTED MEDIA TYPES   | REPORTING  |  |
| <p>Cisco network devices with the following operating systems:</p> <ul style="list-style-type: none"> <li>IOS devices (versions 12 - W, T, JAL, SE , 15 - T, JD, M, E)</li> <li>NX-OS (versions 5, 6, 9)</li> <li>ASA (version 9)</li> <li>AIRCAP</li> <li>AVM FRITZ!Box</li> </ul> <p>For information about support for other devices and platforms, please contact Blanco.</p>  | <ul style="list-style-type: none"> <li>Automatically generates a digitally signed erasure report after each erasure</li> <li>Report details include router or switch serial numbers and other hardware specifics</li> <li>Enables saving reports locally or sending them through the network to the Blanco Management Console (BMC)</li> <li>Tamper-proof erasure reports ensure compliance with data privacy and protection standards and regulations</li> <li>Reports available in CSV, PDF and XML formats</li> </ul> |  |
| SYSTEM REQUIREMENTS   | AUDITING   | LANGUAGE SUPPORT   |
| <ul style="list-style-type: none"> <li>Windows 10 or Windows Server 2016</li> <li>Blanco Management Console—Cloud account or local BMC installation</li> <li>Licenses for BNDE and an active internet connection (for BMC—Cloud)</li> </ul>   | <ul style="list-style-type: none"> <li>Produces a 100% certified and tamper-proof audit trail</li> <li>Digitally signed, tamper-proof reports can be exported to external data bases or into centralized cloud storage (Blanco Management Console)</li> <li>XML, CSV and PDF report formats available</li> </ul>   | <ul style="list-style-type: none"> <li>English</li> </ul> <p>Please ask your Blanco sales representative about non-English language support.</p> |

See what Blanco Network Device Eraser can do: [Request your free ITAD data erasure trial today.](#)