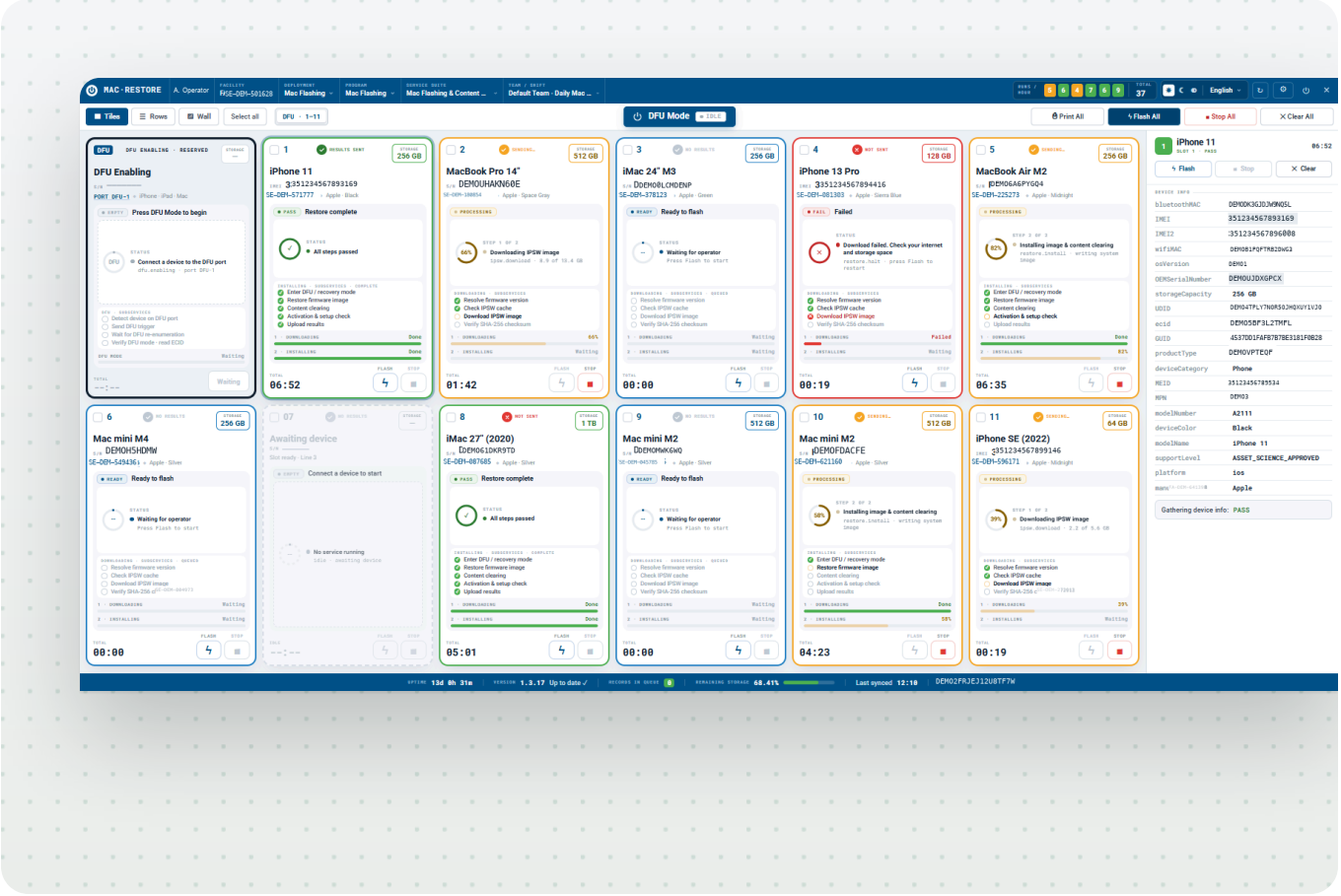
MAC RESTORE

Restore, flash and erase Apple devices at bench scale.

iOS and macOS restoring and flashing on a Mac station. Macs and iOS devices run side by side, the erase is certified to ADISA assurance level 4, and every unit leaves with a certificate anyone can verify.



AUDIENCE

Operations, IT & compliance leads at device processors

PLATFORMS

iPhone · iPad · Mac, on a macOS station

WEB

assetscience.com

AT A GLANCE

The eight questions every buyer asks.

Mac Restore is a restore and erase product. It reinstalls the operating system and clears the device; it does not run a diagnostic suite. The answers below say so plainly.

CERTIFICATE — Yes

Per-device certificate, as a PDF and as a public web page. Lookup by serial or IMEI at verified.assetscience.com/verify, batch PDFs and CSV export.

ADISA CERTIFIED — AAL 4

Certified to **ADISA assurance level 4**, independently tested by the ADISA Research Centre under its Product Claims Test.

TYPE OF WIPE — NIST 800-88

Content clearing with a firmware restore. The operating system is reinstalled from a clean image, the result is verified, and the method is named in the record.

GUIDED USER TESTING — No

There is nothing to guide. The operator connects the device, presses Flash, and answers a DFU prompt when a Mac needs one. The rest is automatic.

TYPE OF TESTS — Not applicable

No functional tests. Mac Restore checks activation and setup state and verifies the installed image. Pair it with a Pro-Diagnostic station when you need a test record.

MAIN FEATURES — 4

Side-by-side Macs and iOS devices, **DFU and recovery** handling, **three floor views** of one run, and a failure that names its reason on the card.

PLATFORMS SUPPORTED — iOS · macOS

Restores iPhone, iPad, MacBook, iMac and Mac mini. Runs on a macOS station. No proprietary hardware required.

DATA ANALYTICS AND API — REST

Every run lands in Control Center as a device record: identifiers, method, outcome and operator. Reachable through the REST API and CSV or Excel export.

One run, six steps, every device

STEP 1
Enter DFU / recovery
Device placed in the mode a restore needs.

STEP 2
Restore firmware
Clean image downloaded and installed.

STEP 3
Content clearing
User data removed with the reinstall.

STEP 4
Activation & setup
State checked and recorded.

STEP 5
Verify SHA-256
Installed image checked against its checksum.

STEP 6
Upload results
Record sent to Control Center.

What we do not do. Locks are reported, never removed or bypassed. A device with Activation Lock or Find My enabled is recorded as locked and routed by your workflow.

WHAT IT DOES

A connected device goes through the full restore pipeline without an operator babysitting each step.

Enter DFU, restore firmware, clear content, check activation and setup, verify, upload the result. Macs and iOS devices run side by side on the same bench.

Mac Restore was built for restoring Apple hardware: **MacBook, iMac, Mac mini, iPhone and iPad**. The device is handled in recovery mode. Its operating system is reinstalled from a clean image, the install is verified against a SHA-256 checksum, and the outcome is uploaded as one record per device.

Apple devices that need a clean operating system include Macs, which a Pro-Diagnostic Desktop station cannot reinstall. iOS flashing at a Pro-Diagnostic Desktop station covers iPhone and iPad. Mac Restore runs on a Mac and covers Macs as well.

A Mac is never erased by Pro-Diagnostic PC & Mac. That product diagnoses the machine; Mac Restore does the Mac wipe. The two share one Control Center, so a unit tested on one station and restored on another has one history.

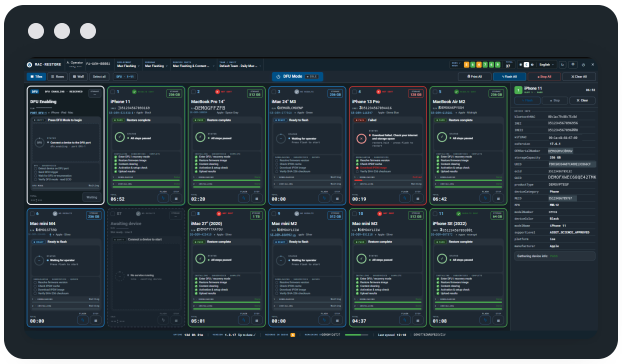


FIG. 1 Mac Restore → Tiles, dark mode. Eleven slots at once, each showing exactly which step it is on, with the device information rail on the right. Identifiers shown are synthetic.

- **Macs and iOS devices in parallel.** A MacBook Pro and an iPhone 13 Pro occupy adjacent slots and run their own pipelines.
- **A failure names its reason on the card.** A download error or a restore error is written on the tile, with the next action, not in a log file.
- **Two-phase progress per slot.** Downloading and installing are shown separately, with a percentage and the sub-step in progress.
- **Per-slot elapsed time and a total-time strip.** The supervisor sees how long each unit took and how long the run has been going.

RESERVED SLOT

DFU enabling

A dedicated port puts a Mac into DFU mode: detect on the DFU port, send the trigger, wait for re-enumeration, read the ECID. The operator presses one button.

FIRMWARE

Image cache

The station resolves the firmware version, checks its local image cache and downloads only what is missing. Remaining storage is shown in the status bar.

BENCH CONTROLS

Flash All · Stop All · Print All

Start, stop or print the whole bench from the toolbar, or select a subset of slots and act on just those.

THE STATION EXPERIENCE

Three views of the same floor, because a bench of four and a bench of forty-eight are different problems.

Tiles give each slot its step checklist. Rows compress the floor to one line per slot. The wall sorts everything by what needs a human next.

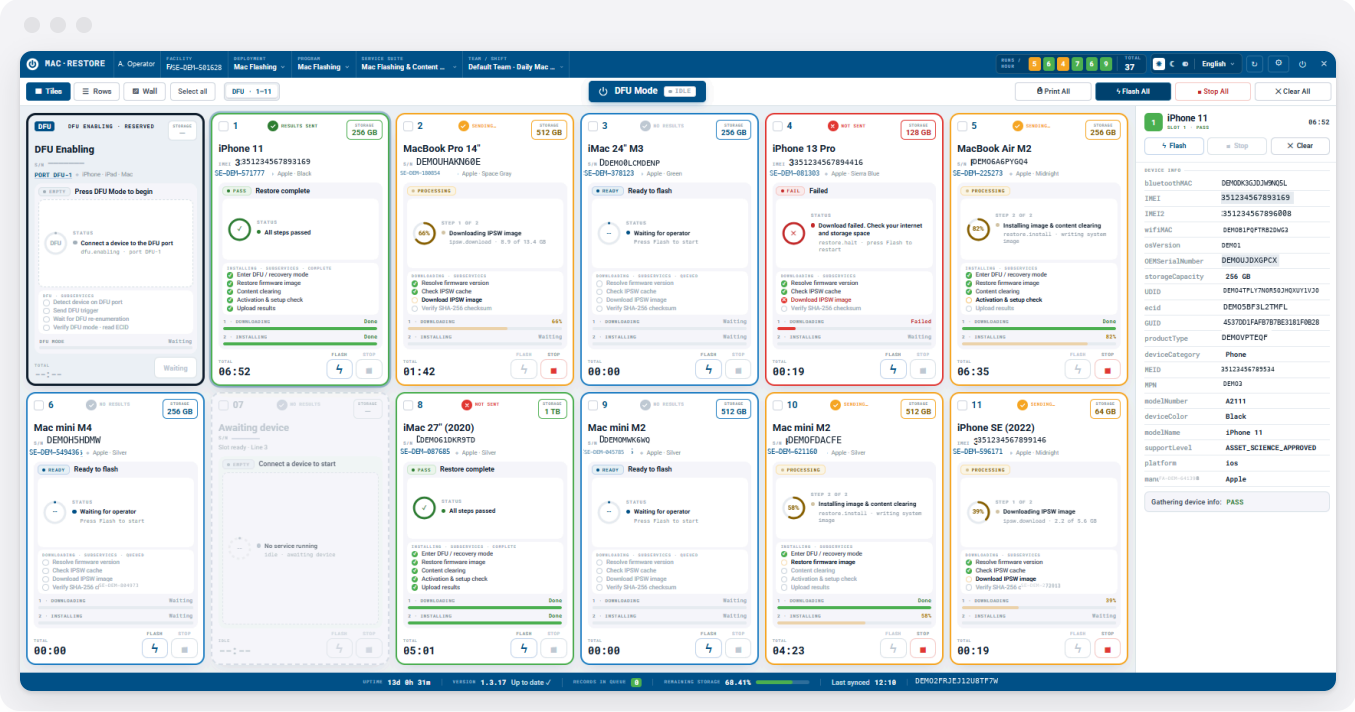


FIG. 2 Mac Restore → Tiles, mid-run. Mixed Macs and iPhones restoring in parallel, with per-slot progress and elapsed time. Slot 4 has failed a download and says so on the tile, with the instruction to press Flash to restart.

Tiles is the operator's view. Each slot carries the device name, serial and IMEI, storage size, a status line in plain words, the six-step checklist with the current step highlighted, and the two progress bars. The right-hand rail shows the selected device's identifiers: IMEI, UDID, ECID, model number, MPN, OS version and storage.

Colour carries state across every view. Green is complete and sent, amber is processing, blue is ready and waiting for the operator, red is failed. An empty slot is drawn dashed and labelled Awaiting device.

The status bar at the bottom reports **uptime, version, records in queue, remaining storage and last sync**. A record that cannot be uploaded yet waits in the queue and is sent when the network returns, so a station keeps working through an outage and nothing is lost.

- **Runs per hour** and the day's total sit in the header for the shift.
- **Select all** or pick slots, then Flash, Stop or Clear the selection.
- **Five sign-in languages**: English, Spanish, French, Dutch, Japanese.

ROWS AND WALL

One line per slot, or sorted by who acts next.

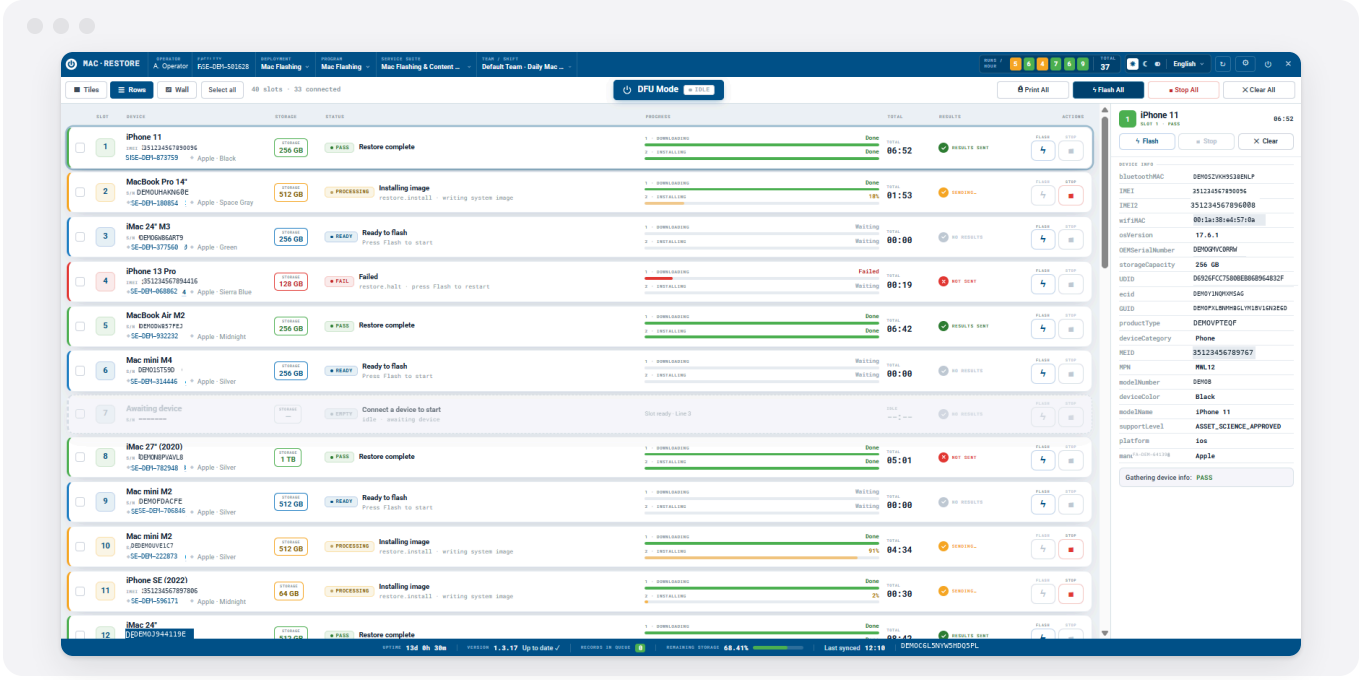


FIG. 3 Mac Restore → Rows, light mode. Forty-eight slots, thirty-three connected, one line per slot with the two-phase progress bars, total time and results-sent state. The density a supervisor wants when the bench is full.

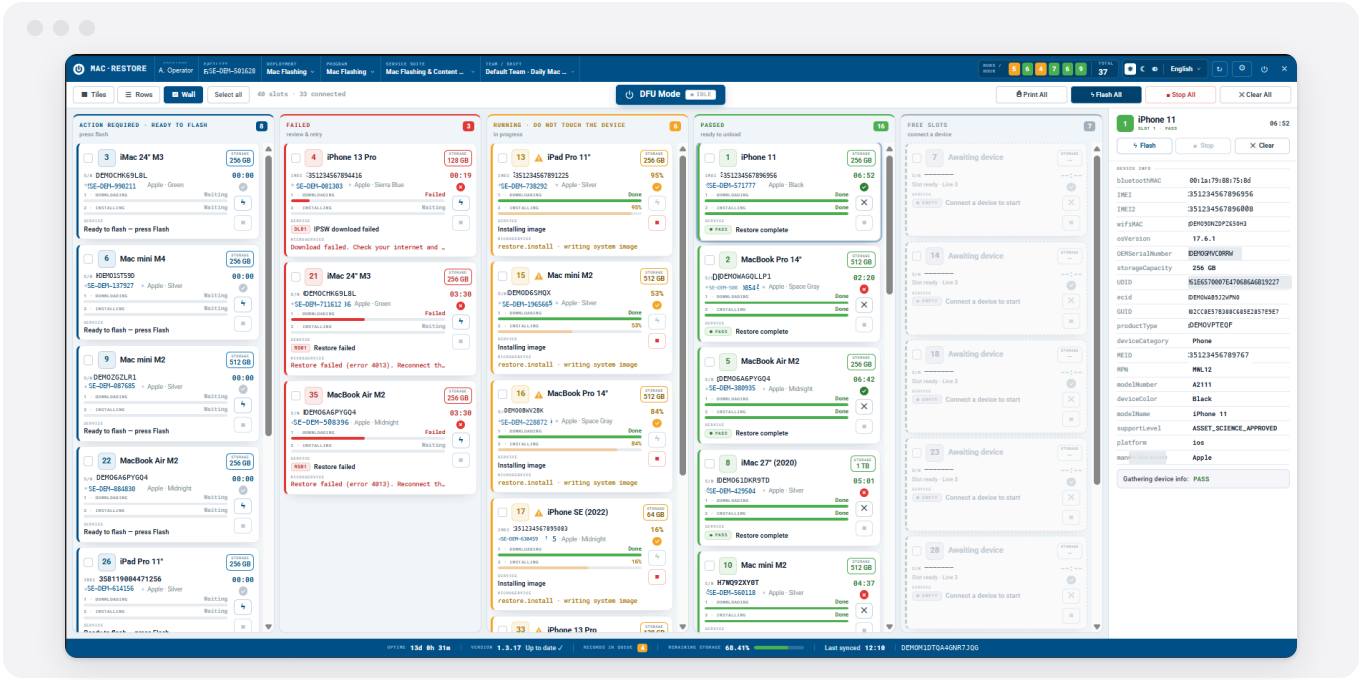


FIG. 4 Mac Restore → Wall. The bench sorted into five columns: action required, failed, running, passed and free slots. The running column is labelled “do not touch the device”, so a new operator knows which units are mid-restore before reaching for a cable. Failures name themselves, with a download error and a restore error here.

ERASURE & CERTIFICATION

Erasure you can hand to an auditor.

The erase is verified rather than assumed, and the method used is named in the record. The certificate is published at the device level, so a buyer can check a specific unit instead of taking a batch claim on trust.

AAL 4
ADISA assurance level
Product Claims Test, ADISA Research Centre

800-88
NIST SP 800-88 compliant
Method named on the report

1
Certificate per device
PDF and public web page

Certification. Pro-Diagnostics and MacRestore are certified to ADISA assurance level 4, independently tested by the ADISA Research Centre under its Product Claims Test. Certification applies to these products; Pro-Diagnostic PC & Mac is not certified and we make no certified-erasure claim for computers it erases.

Method. The device is erased and its operating system reinstalled from a clean image. The content-clearing method is stated on the certificate, and the installed image is verified against its SHA-256 checksum before the result is uploaded. A restore that does not complete is recorded as failed, never as a pass.

Public lookup. Anyone can check a device, without an account. Scan or type a serial, IMEI, MEID or GUID at verified.assetscience.com/verify. A device nobody processed comes back Not Found rather than a reassuring blank.

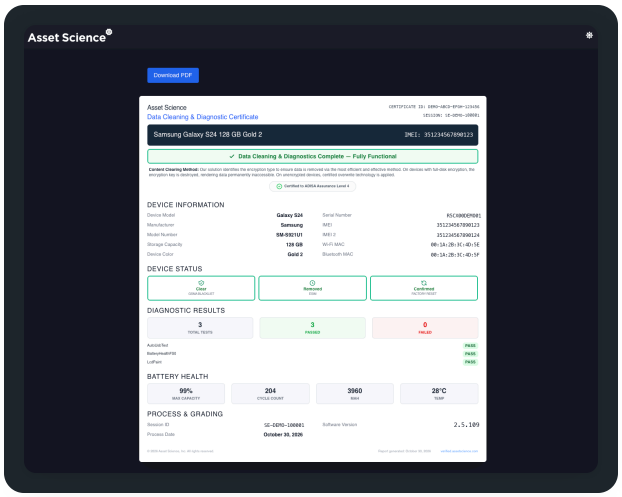


FIG. 5 verified.assetscience.com → Certificate. The public certificate page: device information, content-clearing method, ADISA assurance level 4 mark, device status and a Download PDF button. Sample record shown.

YOU DECIDE WHAT IS PUBLIC

Publication is set **per customer account** in Control Center. Public search, public certificate links and public PDF download are three separate switches.

EVIDENCE BY THE BATCH

Export a scanned batch to CSV from the lookup screen, look up a **CSV of up to 30,000 identifiers**, and generate certificate PDFs in batch. Certificate links travel inside exported reports.

REPORTING & CONTROL CENTER

Results land in Control Center with everything else.

The station signs in against the same Control Center tenant as the rest of the bench. Programs are defined once in the web platform and every Mac Restore station follows them.

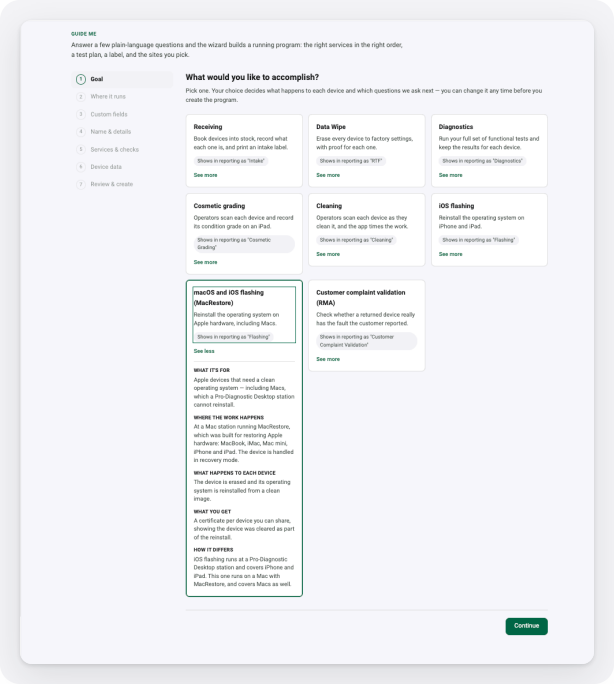


FIG. 6 Control Center → Guide Me → Configuration Wizard. A program starts as a plain-language goal. The macOS and iOS flashing (MacRestore) card is expanded, showing what it is for, where the work happens and what you get.

One program, every station. In Control Center the wizard turns a goal into a running program: the right services in the right order, a label, and the facilities and deployments it runs at. Mac Restore picks the program up at sign-in, which is why the header of every screenshot in this paper carries a facility, a deployment, a program and a team.

One record per device. Each run is stored against the unit's identifiers: serial, IMEI, UDID, ECID, model number, MPN, OS version and storage. The record carries the content-clearing method, the outcome, the operator and the time, and shows in reporting as Flashing.

- **Per-unit history** in Device History, with the public certificate one click away when publication is on.
- **Operator audits and performance dashboards**, with UPH tracked by operator and by bench.
- **Scheduled reports** emailed on your cadence, and full export to CSV and Excel.
- **REST API** for getting data in and out, with licence keys scoped to a tenant, a facility or a single deployment.

1
Define
Pick the macOS and iOS flashing goal in Control Center and choose where it runs.

2
Sign in
The Mac station signs in and loads the program for its deployment.

3
Restore
Devices are flashed and cleared in parallel; results queue if the network drops.

4
Report
Records, certificates and exports are available to your team and your API.

CERTIFICATION

A record nobody outside your building can read is an assertion.

Every device Mac Restore processes can be looked up by serial or IMEI on a public page, by your buyer, your client's auditor, or the person who ends up owning the device. The erase behind it is certified to ADISA assurance level 4.

See it on your own Macs and iPhones.

Start a free trial and run Mac Restore on a Mac in your facility, against your own Control Center tenant. No proprietary hardware required.

FREE TRIAL
onboarding.assetscience.com

PUBLIC CERTIFICATES
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Screenshots are from production builds; device identifiers, operator names and customer data shown are synthetic. Apple, Mac, MacBook, iMac, Mac mini, iPhone and iPad are trademarks of Apple Inc. Product names and marks belong to their respective owners.