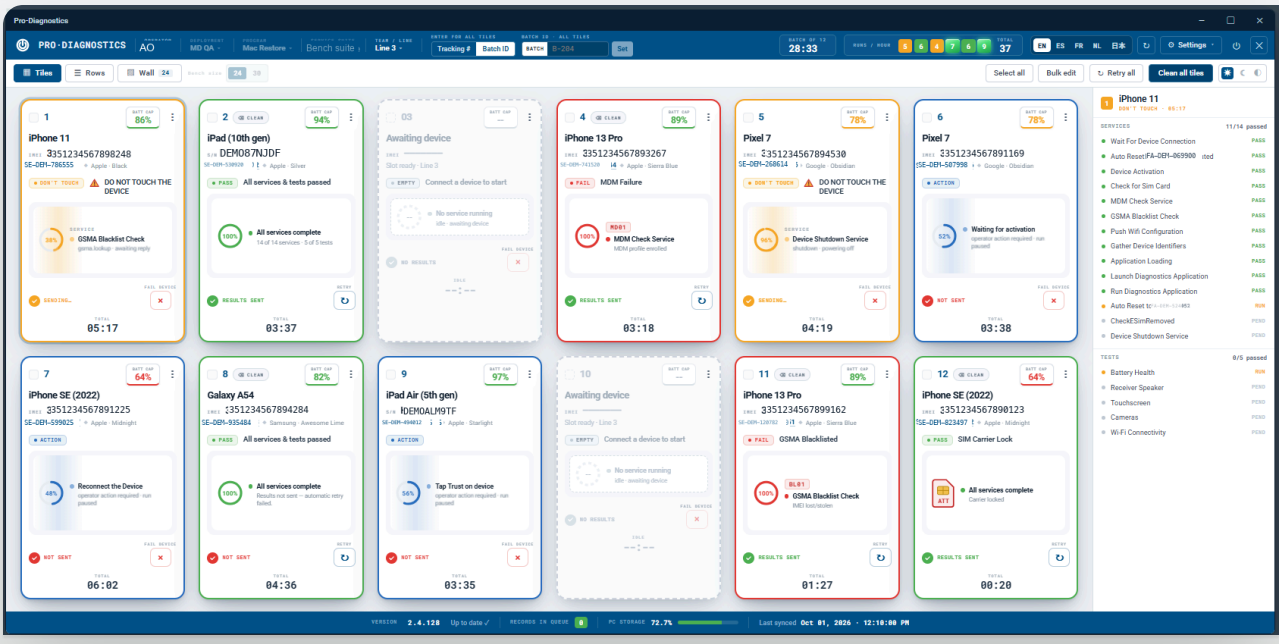
THE ASSET SCIENCE PLATFORM

Run the whole floor from one platform.

Receive, diagnose, erase, grade, certify and report on iOS, Android, Mac and PC from the same bench, under one workflow, with one record per device. Built inside a high-volume refurbishment operation, not a lab.



AUDIENCE

Operations, IT & compliance leads at device processors, carriers, insurers and ITAD firms

COVERS

Diagnostics · Testing · Shop floor · API · Certification · Data wipe

WEB

assetscience.com

EXECUTIVE SUMMARY

One record per device, from the loading dock to the marketplace.

Receiving, diagnostics, erasure, grading and certification are not six tools that exchange spreadsheets. On this platform they are one record, moving through one workflow, written to one Control Center and leaving again by certificate, export or API. The station apps run on the Windows PCs, Macs and iPads you already own. Locks are reported, never bypassed. Erasure on Pro-Diagnostics and MacRestore is certified to ADISA assurance level 4; on PCs it follows NIST 800-88 methods with a per-drive erase report.

CONTENTS

01 **At a glance** 3
The eight questions every buyer asks

02 **The platform** 4
One Control Center, 27 modules, four hosts

03 **Diagnostics and testing** 5
133 Android · 83 iOS · 23 Mac · 25 PC

04 **Device coverage** 7
Tested, erased, graded, restored per platform

05 **The shop floor** 8
Stations, workflow, audits, UPH, labels, SKUs

06 **Data wipe** 10
ADISA AAL 4, NIST 800-88, verification limits

07 **Certification** 12
Public lookup, PDF, batch, three switches

08 **Data and reporting** 13
Per-unit history, dashboards, exports

09 **API integration** 14
REST, scoped keys, GSMA, automation flows

10 **The product line** 15
Ten products, one Control Center

11 **Getting started** 16
A free trial on a station in your facility

133
Android tests
83 on iOS

23 · 25
Mac · PC tests
Guided and automatic

27
Platform modules
One Control Center

AAL 4
ADISA assurance level
Pro-Diagnostics · MacRestore

12M+
Devices a year
800+ installs in the field

7
Operator languages
EN · ES · FR · DE · IT · JA · NL

How to read this paper. Pages 3 to 14 describe the platform as a whole and name the product that holds each capability. Page 15 lists the ten products; each has its own whitepaper with the full detail.

AT A GLANCE

The eight questions every buyer asks, answered for the whole platform.

Each answer names the product that holds it. Certification claims are stated at their scope, with the certified products named.

CERTIFICATE

Yes

One certificate per device: a PDF, a public web page anyone can open by IMEI, serial, MEID or GUID at verified.assetscience.com/verify, and batch CSV or batch PDF. Held by Public Web Certification; issued from Pro-Diagnostic Desktop, Mac Restore and Pro-Diagnostic PC records.

ADISA CERTIFIED

AAL 4

Pro-Diagnostics and MacRestore are certified to ADISA assurance level 4, independently tested by the ADISA Research Centre under its Product Claims Test. Pro-Diagnostic PC & Mac is not ADISA certified: NIST 800-88 methods, per-drive erase report.

TYPE OF WIPE

NIST 800-88

Content clearing on iOS and Android, **Express Connect** for Android 16+ with no USB debugging, **smartphone flashing**, **Mac wiping** with a firmware restore, and on PCs **Purge or Clear per drive** with sampled read-back. The method is named on every report.

GUIDED USER TESTING

Yes

Guided tests appear **one screen at a time, in a fixed order**, with the instruction on screen, in seven operator languages. Automatic tests run with no operator action. Pro-Diagnostic Desktop on phones; Pro-Diagnostic PC & Mac on computers.

TYPE OF TESTS

133 · 83 · 23 · 25

133 Android, 83 iOS, 23 Mac and 25 PC tests across audio, battery and power, buttons, camera, connectivity, display and input, sensors and system, plus lock and fraud detection on every phone run.

MAIN FEATURES

4

Multi-device stations with a workflow manager across benches · **operator audits and UPH** built into the product · **certified erasure** with a public certificate · **one Control Center** that defines programs once for every station.

PLATFORMS SUPPORTED

iOS · Android · Mac · PC

Tests iOS, Android, Mac and PC; restores and erases iOS and macOS; receives Apple Watch Series 1 to 6. Station apps run on **Windows, macOS, iPad and a bootable Linux stick**. No proprietary hardware.

DATA ANALYTICS AND API

REST

Per-unit history, operator audits, UPH dashboards and day-vs-day comparison in Control Center. Every record reachable through the **Back-Office REST API**, CSV and Excel export with a column picker, and scheduled reports.

7,000+
Android models
90 iOS models · 4,500 variants

4
Station hosts
Windows · macOS · iPad · Linux stick

30,000
Identifiers per bulk lookup
From one CSV

47
Export columns
CSV · JSON · Excel

What we do not do. We report locks: Apple ID and Find My, GSMA Lost & Stolen, FRP, passcode, BIOS password, Absolute, TPM. We do not remove or bypass them.

THE PLATFORM

Station apps on the floor, one Control Center behind them, and the record leaves by certificate, export or API.

Control Center is where you decide what happens to a device. The station apps carry it out on the machines you already own.

STATION APPS · ON THE BENCH

Pro-Diagnostic Desktop
iOS and Android diagnostics and erasure. Windows or macOS station.

Mac Restore
iOS and macOS restore, flash and erase. macOS station.

Pro-Diagnostic PC & Mac
Computer diagnostics and drive erase. Signed Mac app; bootable Linux stick on PCs.

Grading & Cleaning
Scan-to-grade on an iPad at the bench.

Apple Watch Receiving
Intake over cable, Series 1 to 6.

CONTROL CENTER · 27 MODULES

Defined once. Followed by every station.

Web-based, multi-facility. Programs start as plain-language goals and every station signs in to the tenant and runs what it is told.

Configuration Wizard · Programs · Test suites per platform · Fail codes · Custom fields · SKU groups & SKU manager · Facilities · deployments · shifts · teams · Operator audit levels · Workstation management · Label printing & designer · Device scanning · Data import · Automation flows · GSMA blacklist · Device history · Reporting & BI · API keys · Role-based access

OUTPUTS · WHAT LEAVES THE BUILDING

Public certificates
Per-device page, PDF and batch at verified.assetscience.com/verify.

Reporting & dashboards
Per-unit history, operator audits, UPH, day-vs-day.

REST API & export
Scoped keys, CSV and Excel, scheduled reports.

Labels & integrations
Asset labels at the bench; NetSuite, MDM, ERP and WMS.

A program starts as a goal, not a script. The Configuration Wizard turns receiving, data wipe, diagnostics, grading, cleaning, flashing or complaint validation into the services the stations run, in a fixed order, at the facilities and deployments you name. A default config bundle gets a new tenant onto the floor fast.

No proprietary hardware. The platform is software that drives equipment you can buy from anybody: the bench PC, the Mac, a barcode scanner, a label printer, USB cables. No robot, no rig, no fixture.

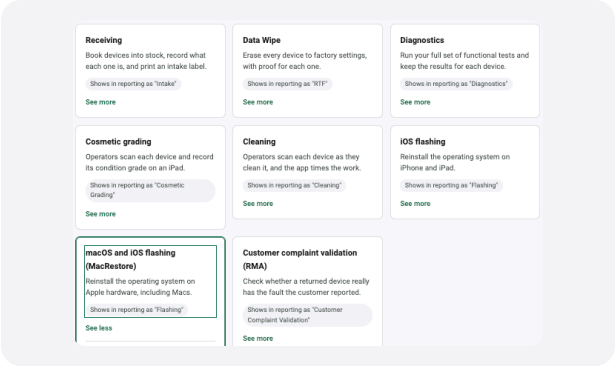


FIG. 1 Control Center → Guide Me → Configuration Wizard, step 1. Plain-language goals, each saying what it is for and how it shows in reporting.

DIAGNOSTICS AND TESTING

A device is plugged in, identified, and put through the suite its program calls for.

Automatic tests run with no operator action. Guided tests are handed to the operator one screen at a time, in a fixed order, with the instruction on screen. The result is one record per device.

133
Android tests
83 on iOS

23 · 25
Mac · PC tests
Pro-Diagnostic PC & Mac

7,000+
Android models
90 iOS models · 4,500 variants

7
Operator languages
EN · ES · FR · DE · IT · JA · NL

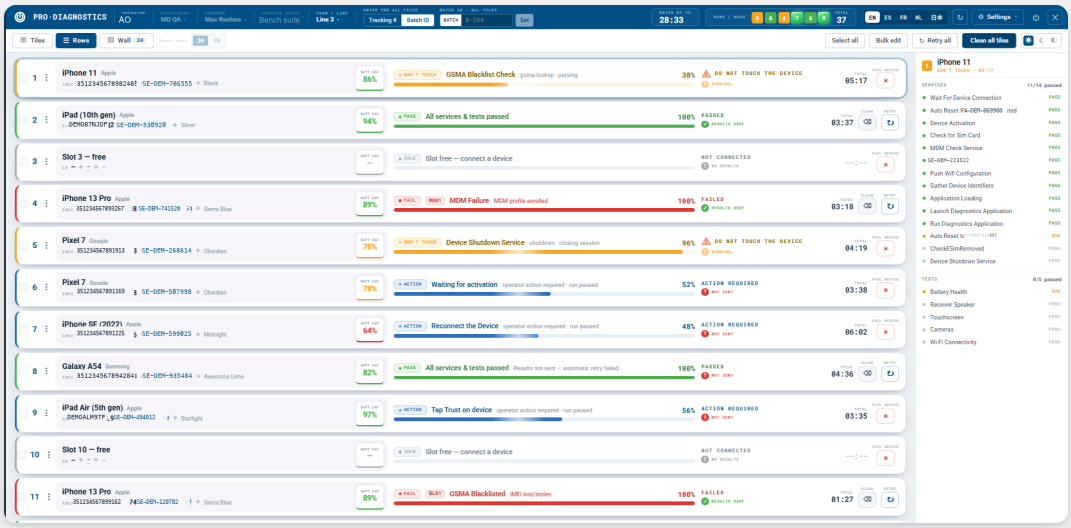


FIG. 2 Pro-Diagnostics Desktop → Rows. Twenty-four slots on one station, one line per device, with the current service and its progress on each: a GSMA check running, an MDM failure, a GSMA blacklist hit, action required, passed. Identifiers shown are synthetic.

Where a test can be done by the machine, it is. Battery health, storage, OS version, carrier, lock state and SIM detection are read without touching the device. The operator is only interrupted when a guided test needs a hand, and the card says so.

Several devices on one station. Each slot runs its own program and shows its own service state, battery capacity and elapsed time. A failure names its service and reason on the card, so the operator reads "GSMA Blacklisted · IMEI lost/stolen" on the slot, not a code to look up.

- **Guided tests measure, not ask.** Depth readings, button counters and signal values are shown before anyone is asked to judge.
- **Hardware a device does not have is skipped**, never failed, and recorded as skipped.
- **A fail opens the fail-code picker**, so the reason travels with the record. Overrides are recorded as overrides, not as passes.
- **Windows or Mac, same suite**, same fail codes, same record format. Per-model inclusion and exclusion is set per test in Control Center.

GUIDED TESTS · LOCK AND FRAUD DETECTION · COMPUTERS

Guided tests that measure. Locks that are reported, never bypassed.

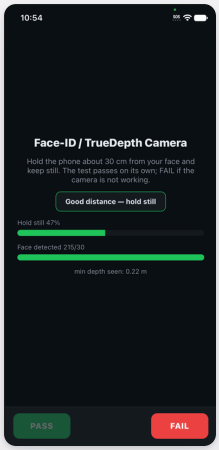


FIG. 3 On-device → Face ID. Hold-still percentage, frames detected and minimum depth are reported before anyone is asked to judge.

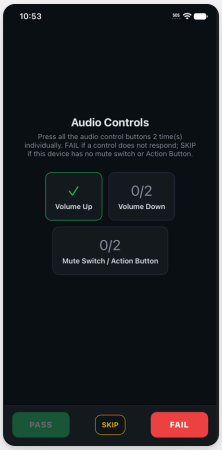


FIG. 4 On-device → Audio controls. Per-button counters, and a Skip button: a device without a mute switch is skipped, not failed.

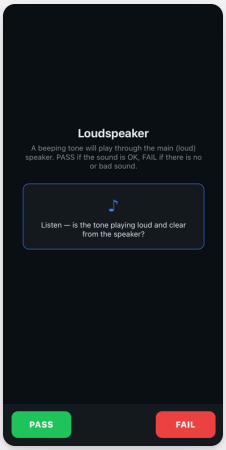


FIG. 5 On-device → Loudspeaker. One instruction per screen. Nothing to interpret, nothing to remember.

Checked during the run, not as a separate pass.

DETECTION	WHAT IS REPORTED	WHERE	STATUS
Apple ID lock · Find My (FMIP / FMAP)	Activation lock and Find My state, read during identification and shown on the card.	iOS · Mac	Reported
GSMA Lost & Stolen	IMEI checked against the GSMA blacklist; a hit fails the slot with the reason named on it.	iOS · Android	Reported
FRP · passcode · fake device · non-OEM parts	Factory-reset protection, passcode and lock-screen state, fake-device detection, non-OEM replacement parts, root or jailbreak, SIM, SD and eSIM presence.	iOS · Android	Reported
BIOS password · Absolute · TPM	Locks that block resale on a PC, worded as the action each blocks.	PC	Reported
Lock removal or bypass	Not offered. A locked device is recorded as locked and routed by your workflow.	All	Not done

MAC · 23 TESTS

A signed macOS app, run on the Mac itself.

Audio, camera, display and input, battery and power, connectivity and ports, memory, storage and thermals, sensors and identity. Any Mac on macOS 13 or later. The Mac is never erased by the diagnostic app; Mac Restore does the wipe.

PC · 25 TESTS

A bootable Linux stick. The installed OS is never trusted or needed.

The PC boots the stick straight into the app in under 90 seconds. Adds WWAN and GPS, orientation sensors and the BIOS, Absolute and TPM lock check. Every internal drive is erased in the background while the operator tests.

DEVICE COVERAGE

Phones, tablets, Macs, PCs and watches, from the same bench.

Most platforms in this category do mobile and stop. Running computers and phones through one workflow, one record and one report is the difference between a tool and an operating platform.

PLATFORM	PRODUCT	TESTED	ERASED	GRADED	RESTORED / FLASHED	ADISA AAL 4
iOS & iPadOS	Pro-Diagnostic Desktop	83 tests	Content clearing, flashing	Yes	iOS flashing on PDD or Mac Restore	Certified
Android	Pro-Diagnostic Desktop	133 tests	Content clearing, Express Connect 16+, flashing	Yes	Smartphone flashing	Certified
macOS · restore	Mac Restore	No tests	Mac wipe with firmware restore	Yes	macOS and iOS flashing	Certified
Mac · diagnostics	Pro-Diagnostic PC & Mac	23 tests	Handled by Mac Restore	Yes	Handled by Mac Restore	Not applicable
Windows PC	Pro-Diagnostic PC & Mac	25 tests	Every internal drive, NIST 800-88 methods, verified	Yes	No	Not certified
Apple Watch Series 1–6	Apple Watch Receiving	Receiving over cable	Not supported	SKU group with Watch device type	No	Not applicable

PHONES AND TABLETS

7,000+ Android models. 90 iOS models in 4,500 variants.

USB-C, Lightning and Micro-USB. A test a model cannot run is skipped on that model and recorded as skipped, never as a fail.

COMPUTERS

Any Mac on macOS 13+. Dell, HP, Lenovo and ASUS PCs with UEFI.

Macs are tested by the signed app and erased by Mac Restore. PCs are tested and erased from the same bootable stick; no Windows install is needed.

APPLE WATCH

Series 1 through Series 6, over cable.

Identification and intake records in Control Center alongside every other device. Support for Series 7 and later is built and ready to activate.

One record, whichever station touched it. A Mac tested on a Pro-Diagnostic PC & Mac station and restored on a Mac Restore station has one history in Control Center, with one visit per station.

THE SHOP FLOOR

Six stages, one record, one platform.

A device arrives, and everything that happens to it afterwards is written to the same record. Run the full process on one station or split it across several with the Workflow Manager; combined sessions deliver a single-page result across stations.

1
Receive
Scan the batch label. Operator, program, bench and shift come from the station config.

2
Diagnose
Automatic tests start immediately and keep running while guided tests proceed.

3
Erase
Method selected per device or per drive, then verified before anything is called done.

4
Grade
Cosmetic grade against your own scale, with operator audits sampling the result.

5
Certify
Erase report and device record written, asset label printed at the bench.

6
Report
Everything lands in Control Center and leaves again by CSV or API.

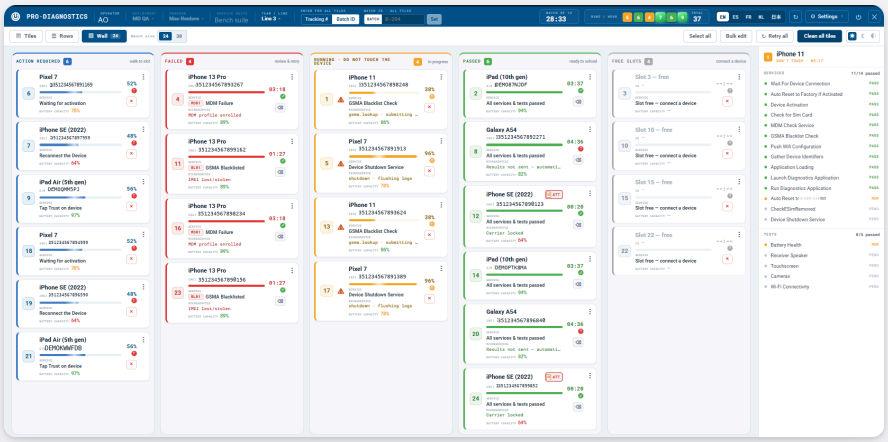


FIG. 6 Pro-Diagnostics Desktop → Wall. The bench sorted by what needs a human next: action required, failed, running, passed, free. A supervisor walks to the right slot instead of scanning every tile. The same wall exists in Mac Restore.

Multi-device stations. Several devices are processed simultaneously on one Pro-Diagnostic Desktop or Mac Restore station, each in its own slot with its own program. Tiles for detail, rows for density, the wall for triage. Bulk edit, retry all and clean all act across the whole bench.

Workflow Manager. A process runs end to end on one station or is split across several: intake on one bench, diagnostics on another, grading on an iPad. Combined sessions merge the visits into one result for the device.

- **Programs per facility and deployment**, with shifts, teams and members in Operation Management.
- **Process names you choose**: intake, diagnostics, content cleared, flashing, cosmetic grading, cleaning, repair depot, complaint validation.
- **Device Scanning** merges the last diagnostic, grading and data-wipe results for a scanned device, or a whole pallet from a CSV.
- **A station keeps working offline.** Records queue on the station and send when the network returns.

OPERATORS, GRADING, LABELS AND YOUR DATA MODEL

How do you know the operator is doing the job and not guessing?

We pioneered operator auditing, and the tooling ships in the platform. An audit is a test whose result the platform already knows, slipped into the normal queue on a normal device, indistinguishable from real work.

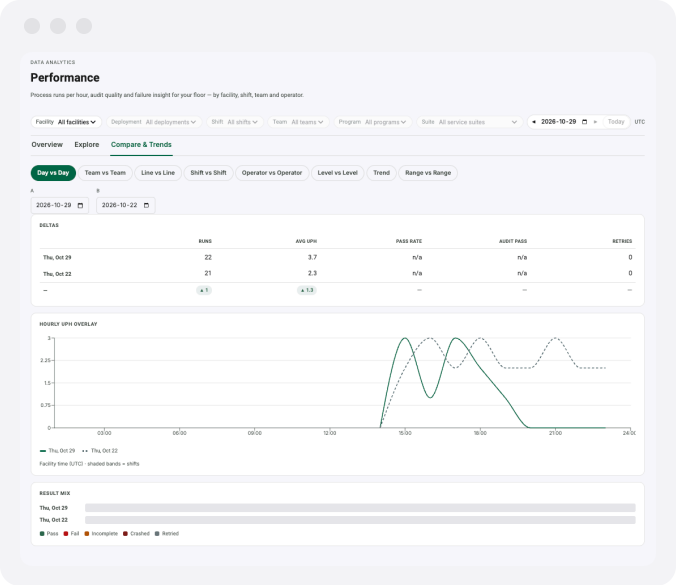


FIG. 7 Control Center → Data Analytics → Performance → Compare & Trends, Day vs Day. Runs and average UPH for two days with the deltas, above both days on the same hourly axis in the facility's own time.

Per audit status, not per person. The ratio of audits to real work is set per operator audit status, so a new hire is audited heavily and a proven operator less. Audit fail sits in the Performance Dashboard beside Processed, Pass rate, Avg UPH, Current UPH, Retries and Incomplete.

UPH you can act on. Average UPH is weighted by active hours and shifts are shaded onto the hourly plot. Eight comparisons, from Day vs Day to Operator vs Operator and Level vs Level. Top fail reasons, top failed tests and top failed audits tell you what to train.

Every action is logged, time-stamped and tied to the operator's ID, so a dispute over a grade traces to a person and a moment.

GRADING APP · IPAD

Scan the device, tap its category, done.

Grading categories defined per customer with their own codes and colors. Double grading where the grade changes the price: the second grader grades blind. First, second and final grade all stay on the record.

LABEL PRINTING

Branded asset labels at the bench.

Templates with barcode and QR previews, Zebra or a system PDF printer, fields mapped from an export or a CSV. The QR code resolves to the device's public certificate. Nothing requires a specific printer.

SKU GROUPS · CUSTOM FIELDS

Your data model, not ours.

SKU groups decide which attributes a device type must carry; the SKU Manager imports and exports them. Custom fields are numeric, string or list, shown at login or at process end, localized per language, and exported beside ours.

Set in two places. Operation Management → Audits sets the audit ratio per facility and per operator audit status. On the test suite itself, operator audits are a 0 to 5 setting beside fail-code display and rapid test. The dashboard refuses to compare two operators at different audit levels without saying so first.

DATA WIPE

What we are certified for, and exactly what that covers.

Certification claims in this market are routinely stretched past their scope. Ours are stated at their scope, with the certified products named.

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

800-88
NIST SP 800-88 Rev. 2
Clear and Purge, named per drive

2883
IEEE 2883-2022
Sanitisation vocabulary

ADISA

Pro-Diagnostics and MacRestore: ADISA assurance level 4.

Independently tested by the ADISA Research Centre under its Product Claims Test. Certification applies to the products named. Pro-Diagnostic PC & Mac is not ADISA certified: NIST 800-88 methods, per-drive erase report.

METHOD	APPLIES TO	HOW IT WORKS	PRODUCT	STANDARD
Content clearing	iOS · Android	Encryption type identified, data removed by the method that fits the device, factory reset confirmed by re-identification.	Pro-Diagnostic Desktop	NIST 800-88
Express Connect	Android 16+	No USB debugging required; cleared from the station without a developer setting.	Pro-Diagnostic Desktop	NIST 800-88
Smartphone flashing	iOS · Android	Firmware rewritten; the device returns in a known state.	Pro-Diagnostic Desktop	NIST 800-88
Mac wipe, firmware restore	macOS · iOS	OS reinstalled from a clean image in recovery mode; installed image verified against its SHA-256 checksum.	Mac Restore	NIST 800-88
NVMe secure erase + verify	NVMe SSD	The drive's own sanitize command, block or cryptographic erase, then read-back.	Pro-Diagnostic PC	Purge
ATA sanitize + verify	SATA SSD · SAS	The drive's native sanitize, cryptographic scramble or block erase.	Pro-Diagnostic PC	Purge
PRNG overwrite, 1 pass + verify	HDD · eMMC · fallback	One pseudorandom overwrite of the full addressable space, where sanitize is unsupported or failed.	Pro-Diagnostic PC	Clear

VERIFICATION, REPORTS AND REFUSALS

The controller saying "done" is not trusted.

A drive that reports successful sanitisation has made a claim about itself. We check it. An unverified drive is recorded as a failed erase, never as a pass.

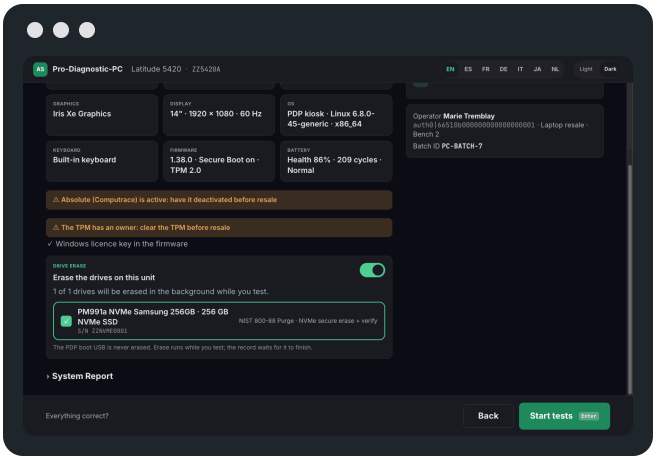


FIG. 8 Pro-Diagnostic PC → Device. One NVMe drive selected for NIST 800-88 Purge, named with its serial before anything is written; Absolute and TPM ownership reported as locks.

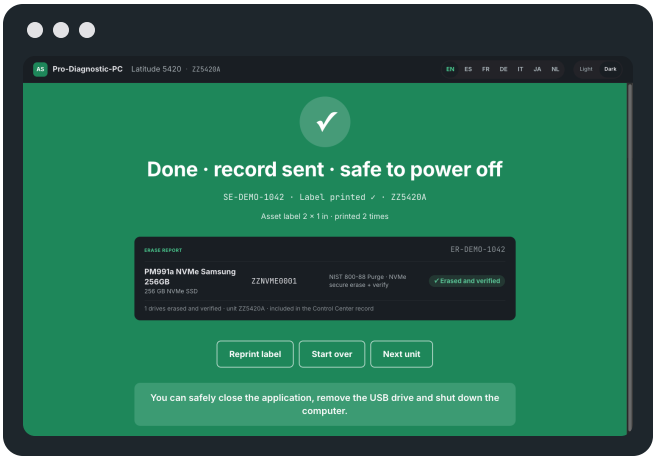


FIG. 9 Pro-Diagnostic PC → Done. Record sent, label printed, and the per-drive erase report: model, serial, method, outcome.

HOW THE READ-BACK WORKS · PC DRIVES

Sampled across the whole disk.

After erasure, the engine reads the drive back at sampled points spread across the whole disk: 1% of the drive by default, up to 4,096 points of 4 MiB each. Any point that still holds recoverable data fails the drive, and a drive that fails verification fails the unit.

AND ITS LIMITS

Sampled, not exhaustive.

An under-wipe in the gaps between sample points is caught with probability, not certainty. We state this plainly because a vendor who claims perfect verification of a multi-terabyte drive in minutes is telling you something that is not true.

When the platform refuses to erase

GATE	BEHAVIOR
No real serial	System, board and chassis serials all placeholders: erase refused.
Low battery	Below 25% on battery, the erase waits for a charger.
Frozen list	Drives fixed before erasure; serials re-checked before writing.
Interruption	Nothing more is erased until an operator chooses: erase again, or record a failure.

What the record keeps

- **Per-drive erase report** with method, outcome and reason, attached to the unit record. A skipped drive is recorded as skipped, with who skipped it.
- **Method named on every phone and Mac record** and on the certificate: content clearing, Express Connect, flashing or firmware restore.
- **Offline queue.** Records are written to disk first and deleted only after Control Center confirms receipt. A station that loses its network keeps working and catches up. A record is never lost.

CERTIFICATION

Anyone can check a device, without an account.

A record nobody outside your building can read is an assertion. Every device you process can be looked up by IMEI, serial, MEID or GUID at verified.assetscience.com/verify, by your buyer, your client's auditor, or the person who ends up owning the phone.

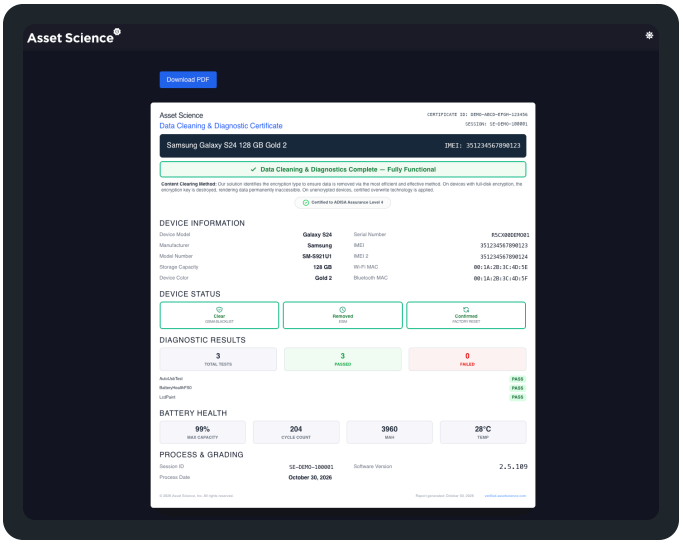


FIG. 10 verified.assetscience.com → Certificate. A Data Cleaning & Diagnostic Certificate: identifiers, content-clearing method, the ADISA assurance level 4 mark, device status tiles, diagnostic results, battery health and a Download PDF button. Sample record shown.

One record, three ways to reach it.

- **Public lookup** by IMEI, serial, MEID or GUID. A device nobody processed comes back Not Found rather than a reassuring blank.
- **Shareable link and PDF**; the QR code on the label resolves to the same certificate.
- **What it shows**: clearing method, ADISA assurance level where the product holds it, GSMA blacklist and factory-reset status, diagnostic results, battery health, process and grading.
- **A failed device is never quietly certified.** A check that did not run shows N/A; a process that failed before the wipe reads Process Failed.
- **Inside and outside match.** The public page is a view of the Device History record in Control Center, not a second copy.

Three switches per customer account, set in Control Center.

CONTROL	WHAT IT ALLOWS
Publish results to public search	Anyone can look up a device you processed by IMEI or serial and see its data-wipe and diagnostic results.
Allow public certificate links	Anyone holding a certificate link can open the certificate page without signing in. Also controls the Public Certificate button in Device History and the links in exported reports.
Allow public PDF download	Anyone holding a certificate link can download the PDF without signing in. A separate switch from the page above, deliberately.

EVIDENCE BY THE BATCH

Nobody clearing a pallet opens one certificate at a time.

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

WHICH PRODUCT ISSUES IT

Stated at its scope.

Certificates from Pro-Diagnostics and MacRestore carry the ADISA assurance level 4 mark. A Pro-Diagnostic PC record feeds the certificate with its per-drive erase report and NIST 800-88 methods, without a certification mark.

DATA AND REPORTING

A grid you work in, not a report you request.

Every run, every operator, every device: queryable, chartable and exportable without asking us for a report. Aggregates are for the plant manager; when a customer disputes a single unit, the platform produces that unit's own record.

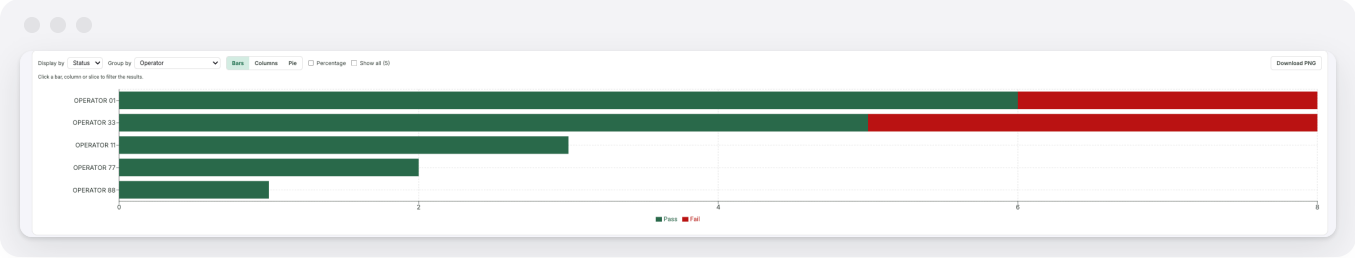


FIG. 11 Control Center → Reporting → Explore, chart band. The rows you are filtering, charted by operator as pass and fail. Clicking a bar filters the grid to it.

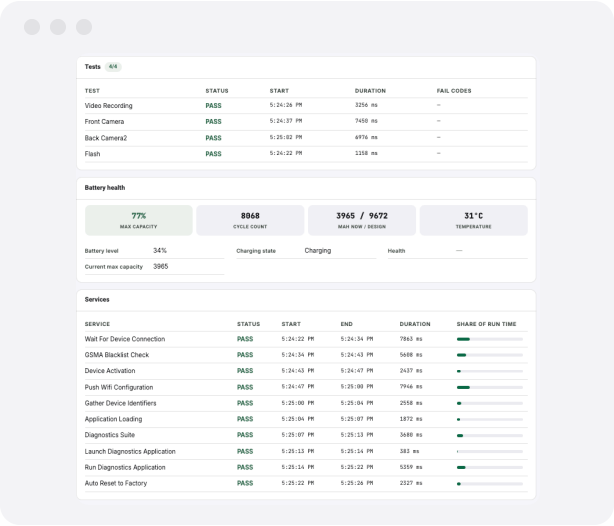


FIG. 12 Control Center → Device History. One device: every test with its duration, battery health tiles, and ten services in the order they ran with each one's share of the run.

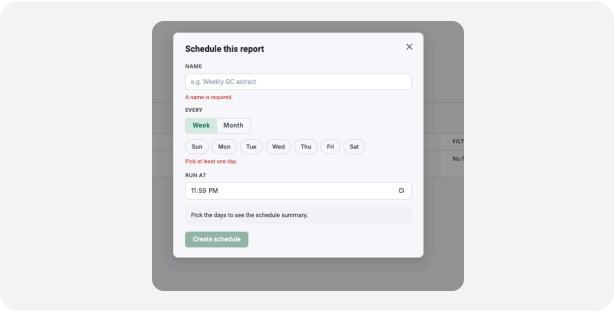


FIG. 13 Reporting → Schedule this report. Weekly or monthly, the days and the run time.

- **Per-unit history**: IMEI, serial, OS, storage, color, region, every test, every service, every override, the erase and the grade. Global lookup by any identifier.
- **Dashboards**: Daily performance indicators per facility; Processed, Pass rate, Avg UPH, Current UPH, Audit fail, Retries, Incomplete.
- **Day vs day** and seven more comparisons, drawn on the same hourly axis with shift bands.
- **Explore**: filter the live grid, chart from it, bulk-search a CSV of identifiers against it.
- **Export**: 47 selectable columns, CSV, JSON or Excel, your custom fields in the same list as ours. Download, email yourself, or email someone without a login.
- **Scheduled reports**, weekly or monthly, on the days and at the time you pick.
- **Data Import Tool** for device lists and manual uploads, validated against your required fields.

No feature gate, no export fee. Full CSV export and the REST API are included on every plan. Your data stays yours.

API INTEGRATION

The record leaves the building as easily as it arrives.

A diagnostic result trapped in a vendor dashboard is worth very little. Everything the floor produces is available by API, by export and by scheduled report.

REST, uniformly. The Back-Office API Suite exposes uniform resource endpoints across the platform's services, authenticated with a bearer token. Data goes in as well as out: third-party systems push records and fields in and pull per-unit history, test results and session data back.

Keys scoped to the part of your operation they should reach. Keys are scoped to a tenant, a facility or a single deployment, so an integration at one site cannot read another.

GSMA Device Check. Lost and stolen checking runs through the same platform, with a free test mode before you commit. Repeat checks inside the caching window are answered from cache and never billed; the usage screen shows the split.

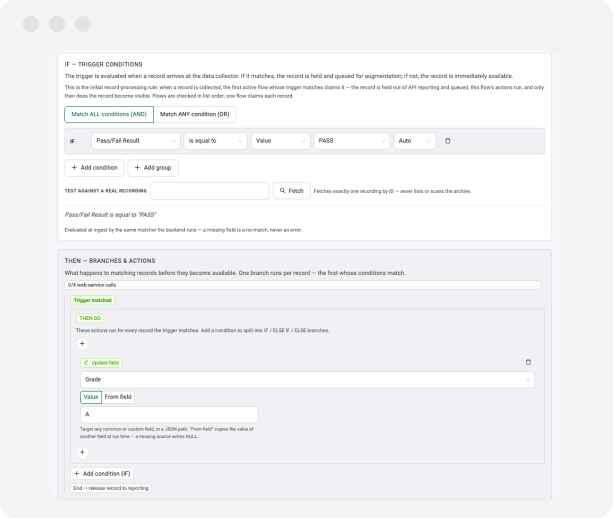


FIG. 14 Control Center → Automation → Edit flow. IF a record's Pass/Fail result equals PASS, THEN update the Grade field, before the record is released to reporting. A flow can also call a web-service connection.

Integration points, at a high level.

INTEGRATION	WHAT IT DOES	WHERE
REST API	Uniform endpoints, bearer-token auth, insert and extract. Keys scoped to tenant, facility or deployment.	Back-Office API Suite
Automation flows	Rules that enrich records after collection, before reporting: IF trigger, THEN update a field or call a web service. First match wins, one flow per record, with a run log.	Control Center → Automation
Web-service connections	Reusable REST calls a flow can invoke: URL, method, bearer or header auth, write-only secret, validated with a sample call before use.	Control Center → Automation
GSMA Device Check	Blacklist and greylist status with the IMEI history behind it. Free test mode; cached answers are not billed.	Station and API
ERP · WMS · NetSuite	Send results to NetSuite as a program option; RMA outcomes pushed to the ERP or WMS that runs your inventory.	Configuration Wizard · RMA module
MDM · Zero-Touch	Approve the diagnostics app automatically on every device through MDM, so the operator does not trust a profile by hand.	Configuration Wizard

THE PRODUCT LINE

Ten products. One Control Center. One record per device.

Every product reports to the same place and reads the same programs. Each has its own whitepaper with the full detail.

IOS & ANDROID · WINDOWS AND MAC

Pro-Diagnostic Desktop (PDD)

Multi-device simultaneous diagnostics at the bench, on a Windows or a Mac station. 133 Android and 83 iOS tests; data erasure certified to ADISA assurance level 4.

See the Pro-Diagnostic Desktop whitepaper

IOS & MACOS

Mac Restore

Full restore platform running on Mac: iOS and macOS flashing, data erasure certified to ADISA assurance level 4, reports and certificates, PDF and web.

See the Mac Restore whitepaper

COMPUTER DIAGNOSTICS & MULTI-DRIVE ERASURE

Pro-Diagnostic PC & Mac (PDP)

Diagnostics and drive erasure for PCs and Macs: a full hardware profile per unit, internal drive erasure using NIST 800-88 methods, a per-drive erase report.

See the Pro-Diagnostic PC & Mac whitepaper

CLOUD PORTAL

Control Center

Web-based management platform: manage your workflow and shop floor with full autonomy. Self-defined parameters and fail codes, custom tests, a default config bundle, role-based access.

See the Control Center whitepaper

ANALYTICS

Data & Reporting Platform

Complete per-unit history, operator audits, performance dashboards and trend analytics. Scheduled automated reports and full data export, CSV and API.

See the Data & Reporting whitepaper

CARFAX FOR PHONES

Public Web Certification

Anyone can look up a device you processed by IMEI or serial at verified.assetscience.com and see its wipe certificate. Shareable link, PDF, batch CSV and batch PDF.

See the Public Web Certification whitepaper

INTEGRATION LAYER

Back-Office API Suite

REST API for getting data in and out, with keys scoped to a tenant, a facility or a single deployment. GSMA Device Check with a free test mode; CSV and Excel export; scheduled reports.

See the Back-Office API Suite whitepaper

SERIES 1 THROUGH SERIES 6

Apple Watch Receiving

Receiving and intake workflows for Apple Watch over cable, with identification and intake records in Control Center. Support beyond Series 6 is built and ready to activate.

See the Apple Watch Receiving whitepaper

QUALITY CONTROL

Manual Grading & Cleaning App

Tablet grading at the bench: scan the device, tap its category, done. Grading categories per customer, double grading where the grade changes the price, UPH and operator auditing.

See the Manual Grading & Cleaning whitepaper

RETURNS MANAGEMENT

RMA Treatment Module

End-to-end RMA processing and treatment tracking with ERP and WMS integration: return authorization workflows, treatment tracking, disposition management.

See the RMA Treatment Module whitepaper

GETTING STARTED

Put it on a bench and see.

Run your own devices through it, on your own floor, against your own grading scale. No credit card and no sales call before you start, and no proprietary hardware to buy.

1

Sign up

Create the account at onboarding.assetscience.com/onboarding/account. The trial starts at your first sign-in.

2

Install a station

Pro-Diagnostic Desktop on a Windows PC or a Mac you already own; Mac Restore on a Mac. Sign in to your tenant.

3

Start from the bundle

A default config bundle gives you programs, suites and fail codes on day one. Adjust them in the Configuration Wizard.

4

Process and look it up

Test and erase a device, open its record in Control Center, then find it at verified.assetscience.com/verify.

IN ONE SENTENCE

One platform for the whole floor, with claims stated at their scope.

133 Android, 83 iOS, 23 Mac and 25 PC tests. Erasure certified to ADISA assurance level 4 on Pro-Diagnostics and MacRestore; NIST 800-88 methods with a per-drive erase report on PCs. Locks reported, never bypassed. A public certificate for every device, on the hardware you already own.

See it on your own devices.

Start a free trial and run the platform on a station in your facility. Pro-Diagnostic PC & Mac, the API Suite, Apple Watch Receiving and the RMA module are set up with us; talk to us when your volume calls for them.

FREE TRIAL
onboarding.assetscience.com/onboarding/account

PUBLIC CERTIFICATES
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Screenshots are from production builds; device identifiers, session IDs, operator names and customer data shown are synthetic. Pro-Diagnostics and MacRestore are certified to ADISA assurance level 4 under the ADISA Product Claims Test; Pro-Diagnostic PC & Mac is not ADISA certified. Apple, Mac, iPhone, iPad and Apple Watch are trademarks of Apple Inc. Product names and marks belong to their respective owners.