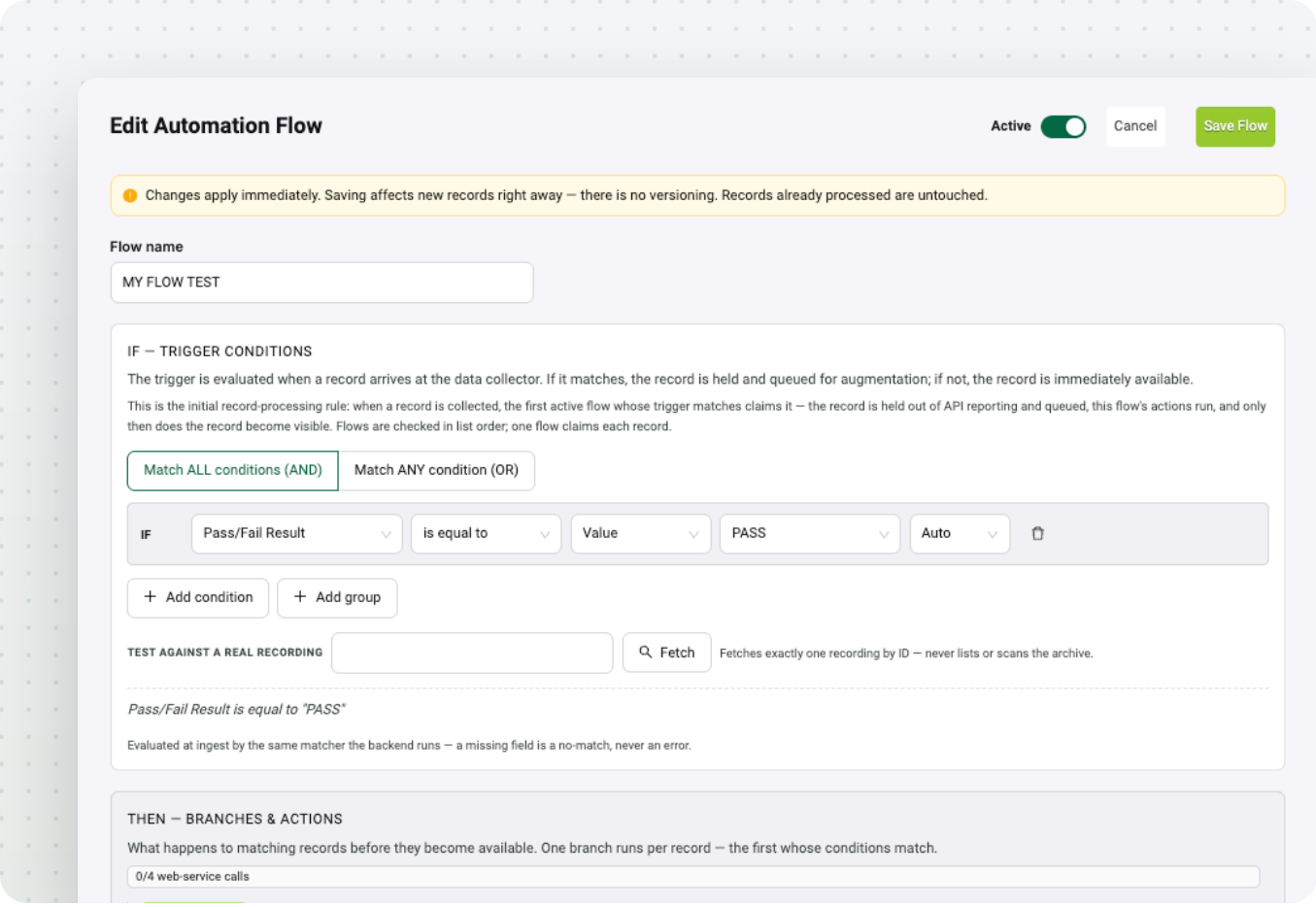
BACK-OFFICE API SUITE

Your data, in and out, without asking us.

A REST API across the platform's services, 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 on your cadence, and automation flows that change a record or send it to your systems before reporting sees it.



AUDIENCE

Integration, IT & operations leads at device processors, carriers, insurers and ITAD firms

INTERFACES

REST · JSON · CSV · Excel · scheduled email

WEB

assetscience.com

AT A GLANCE

The eight questions every buyer asks, answered for an API.

The Back-Office API Suite moves records. It runs no test and erases no drive. Certificates and ADISA assurance belong to the station products that produce them; the API exposes exactly what those products recorded.

CERTIFICATE

Not issued here

The API does not issue certificates. It returns the records that Control Center builds certificates from, including the activation, GSMA and factory-reset status on each run. Certificates themselves are PDF and public lookup at verified.assetscience.com.

ADISA CERTIFIED

Not applicable

No. ADISA assurance level 4 applies to Pro-Diagnostics and MacRestore, the products that perform the erasure. The API carries their records and never changes an erase result.

TYPE OF WIPE

None performed

The API erases nothing. It reports the erase result and method the station recorded: content clearing, Express Connect or flashing from Pro-Diagnostics, and the per-drive NIST 800-88 erase report from Pro-Diagnostic PC.

GUIDED USER TESTING

No

No operator screens. Tests are run at the bench by the station products; the API moves their results and lets your systems react to them.

TYPE OF TESTS

None run

Exposes **every test result with its fail codes** from the 133 Android, 83 iOS, 23 Mac and 25 PC tests, plus service results, grade, overrides and battery health.

MAIN FEATURES

4

Uniform REST endpoints across services. **Keys scoped** to tenant, facility or deployment. **GSMA Device Check** with a free test mode. **CSV and Excel export** with scheduled, emailed reports.

PLATFORMS SUPPORTED

HTTPS

Any client that speaks HTTPS and JSON. Bearer tokens validated against our identity provider for people, licence keys for systems. Automation connections call your own HTTPS endpoints.

DATA ANALYTICS AND API

Yes

The full device record: identifiers, device, session, infrastructure, battery, tests, services, grade and custom fields. **REST**, CSV, Excel and JSON export, scheduled reports by email.

Honest scope. A "No" on five of these eight is the point: this product is the pipe, not the bench. If a claim about a certificate, an erasure standard or a test belongs anywhere, it belongs to Pro-Diagnostics, Pro-Diagnostic PC & Mac or MacRestore, and their own papers make it.

WHAT THE API EXPOSES

One record per process run, holding everything the bench put in it.

Every station product writes the same record shape to Control Center. The API returns that record. What it holds depends on which services the program ran on the device.

GROUP	FIELDS ON THE RECORD
Identifiers	IMEI, IMEI 2, MEID, serial, GUID, ECID, ICCID, Wi-Fi MAC, Bluetooth MAC
Device	Manufacturer, model name and number, product type, OS version, storage, color, region, category
Session	Session ID, cross-system ID, process name, flow and route, start, end, duration, shift, team, operator
Infrastructure	Facility, deployment, computer name, desktop software build
Battery	Level, temperature, charging state, cycle count, health, maximum capacity
Results	Pass, fail or incomplete; every test with fail codes; services run; grade; overrides
Custom fields	Your own keys, defined in Control Center or written by a flow

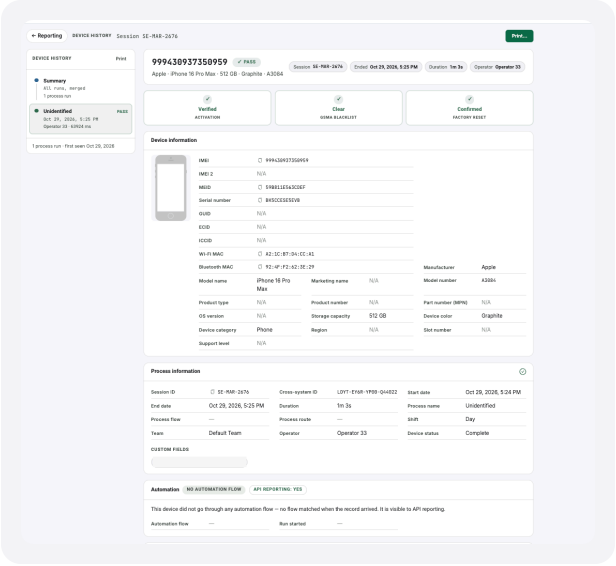


FIG. 1 Control Center → Reporting → Device History. The record header with its activation, GSMA and factory-reset status, the identifier block and the process information. Identifiers are synthetic.

RESULTS AND GRADES

What the bench decided.

The run result is PASS, FAIL or INCOMPLETE, never a bare boolean. Each test carries its own result and fail codes, with the most meaningful code in a dedicated fail-reason field. Activation, GSMA, factory reset and parts check sit on the same record; grading records carry the grade as your own category string.

ERASE REPORTS AND CERTIFICATES

Recorded by the station, read by you.

The erase result and method come from the product that did the work: content clearing or flashing on Pro-Diagnostics, a per-drive NIST 800-88 erase report on Pro-Diagnostic PC. Certificates are built from these records in Control Center and published at verified.assetscience.com; the API reads the record behind them.

PROVENANCE

Automated values never masquerade as bench data.

Every field a flow changes is recorded on the record with the flow name, the time, the original value and the new one, and shown in Device History. Device identity, session IDs and operator identity can never be written by a flow.

DATA IN, DATA OUT

Records arrive from the bench, from a file or from your system. They leave in whatever shape you need.

Getting data in. Most records arrive from the stations by themselves. Three more routes exist for everything else.

- **Identifiers.** Each program declares the minimum identifiers a record must carry, such as the OEM serial number, and the fields that are required before a run is accepted.
- **Custom fields.** Define your own keys in Control Center as list, numeric or string fields, shown at operator login or at process end, with display names per language. They travel on every record and every export.
- **Data Import Tool.** Upload a device list from the CSV template against a facility, deployment, shift, team and program, with file validation before import, or enter one device by hand.
- **REST.** The same resource endpoints that read records also create and update them, so a third-party system can push data in as well as pull it out.

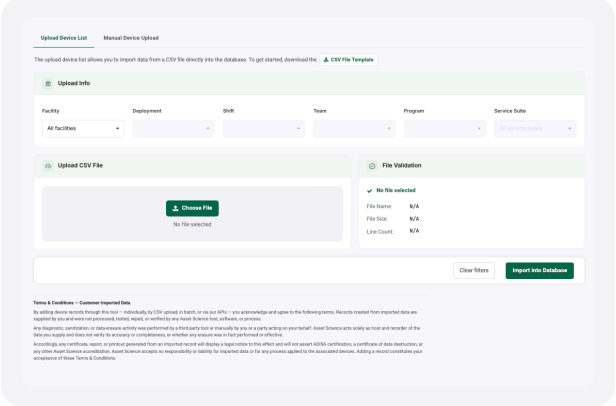


FIG. 2 Control Center → Data Import Tool → Upload Device List. CSV template, target facility and program, file validation, and the notice that imported records carry.

Imported records are marked as imported. A record created from a file or through the API was not processed by an Asset Science tool. Any certificate or printout generated from it carries a legal notice to that effect and asserts no ADISA certification and no certificate of data destruction.

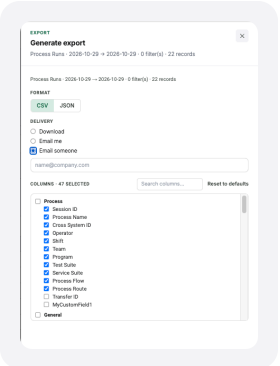


FIG. 3 Reporting → Generate export. CSV or JSON, download or email, 47 columns chosen from the record.

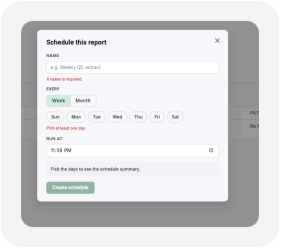


FIG. 4 Reporting → Schedule this report. Weekly or monthly, the days and the time of day.

Getting data out. The record is yours, in five shapes.

- **REST.** List with pagination or fetch one record by its ID, filtered to the tenant, facility or deployment the key is scoped to.
- **CSV and Excel.** Any Reporting view, with the columns you pick, downloaded or emailed to you or to someone else.
- **JSON.** The same export as JSON for a system that would rather parse than import.
- **Scheduled reports.** Name a report, choose weekly or monthly, pick the days and the run time; it arrives by email on that cadence.
- **Export history.** Every generated export is listed with its record count and size, ready to download again or to feed the label printer.

AUTOMATION FLOWS

IF this record, THEN change it or send it, before reporting ever sees it.

Flows are rules your own admins write in Control Center, ordered like mail rules. The first flow whose trigger matches claims the record, runs its actions, and only then releases it to reporting and the API.

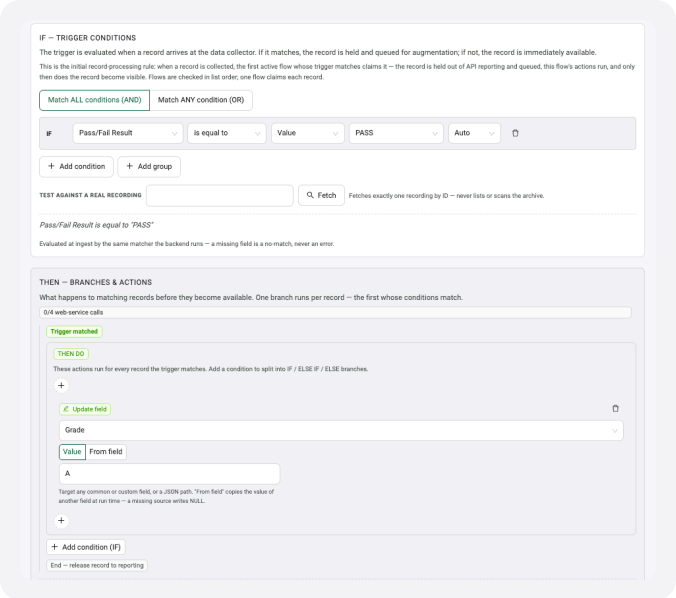


FIG. 5 Control Center → Automation → Edit Automation Flow. IF: Pass/Fail Result is equal to PASS, tested against a real recording. THEN: Update field Grade = A.

IF. Conditions are field, operator and value: is equal to, is not equal to, contains, is greater or smaller than, is null, is not null. Combine them with AND or OR, one level of grouping. Pick from a catalogue of common fields, your custom fields, or any JSON path into the record. Before saving, fetch one real recording by record ID or IMEI and see whether it matches.

THEN. A chain of IF, ELSE IF and ELSE; exactly one branch runs per record. Three actions: **Update field** with a typed value or one copied from another field, **Call web-service**, and **End**. Saved changes reach new records within about a minute.

If the flow fails. Transient errors are retried with backoff. A permanent failure follows the flow's policy: release the record un-augmented and flagged, or block it until a human releases it. Nothing is lost, and a record is never shown half-changed.

Connections are the reusable web-service calls a flow can make: your own HTTPS endpoint, the method, and a Bearer, API-key or Basic header with a write-only secret, masked after save and redacted from logs.

- **Payload you choose.** Custom fields plus the record ID by default, or the full record. Credentials and operator identity are always stripped.
- **Response written back.** Keys from the JSON reply land in custom fields, so an ERP lookup can enrich the record.
- **Validate first.** A sample call shows the server's answer inline; nothing is written to any record.
- **Bounded.** At most four calls per flow. The whole flow re-runs on retry, so your endpoint should be idempotent.

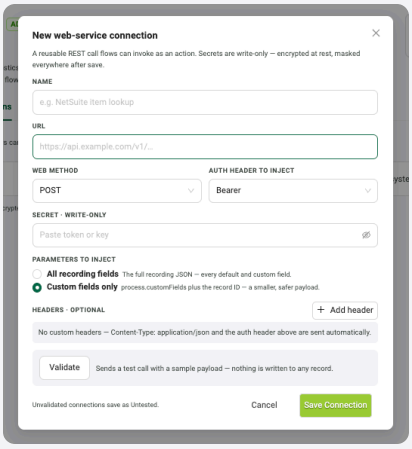


FIG. 6 Automation → Connections → New web-service connection: URL, method, auth header, write-only secret, payload scope, Validate.

GSMA DEVICE CHECK

Lost and stolen checks, with a free test mode before you commit.

Every check looks an IMEI, MEID or ESN up against the GSMA register of lost and stolen devices and returns its blocklist history. Run it from the bench through Pro-Diagnostics, or call it from your own system with a licence key.

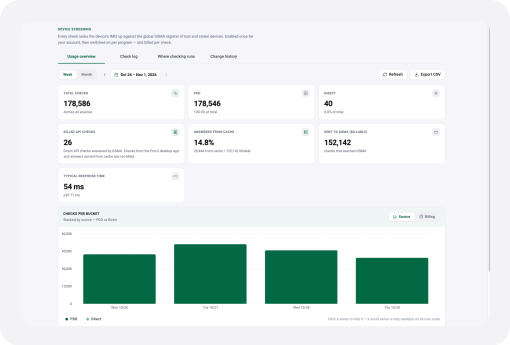


FIG. 7 Control Center → GSMA Blacklist → Usage overview. Checks by source, how many were answered from cache, how many reached GSMA, and the typical response time. Demo data.

```
GET /api/gsma/blacklist?imei=999430937350959&licenseKey=<key>
add &testmode=true for a fixed sample answer, never billed

200 OK
{
  "responsestatus": "success",
  "deviceid": "999430937350959",
  "blacklststatus": "Yes",
  "greyliststatus": "No",
  "imeihistory": [
    { "action": "Block Insert",
      "date": "2021-06-28 21:46:27",
      "reasoncodedesc": "Stolen or Lost" }
  ],
  "manufacturer": "Apple Inc",
  "marketingname": "Apple iPhone SE (A2275)",
  "devicetype": "Smartphone"
}
```

Abridged. Exactly one of imei, meid or esn is given. Blocklist and greylist status are Yes or No; the history is empty for a clean device.

Free test mode. With test mode on, the call returns a fixed sample payload, never reaches GSMA and is never billed. One such call end to end confirms your key, your network path and your parser before any production traffic.

Cache, not invoice. A device already looked up inside the caching window is answered from cache and not billed; only a first-time device is sent to GSMA. The usage screen shows the split, so unit economics are visible rather than inferred from an invoice.

Plain errors. A missing or malformed identifier is a 400, a bad key a 403, an upstream GSMA failure a 500 that is safe to retry once.

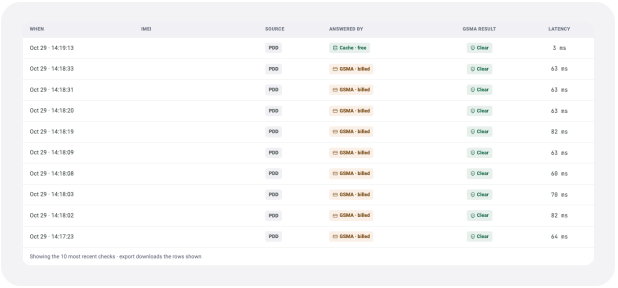


FIG. 8 GSMA Blacklist → Check log. One row per check: source, answered from cache or by GSMA, result and latency. IMEI column blanked; exportable as CSV.

Locks are reported, never removed. A blocklisted device is recorded as blocklisted and routed by your workflow. The check tells you the device's status with GSMA; it does nothing to the device.

KEYS, SCOPING AND INTEGRATION PATTERNS

A key reaches exactly the part of the operation it was issued for.

People sign in with a bearer token validated against our identity provider. Systems use a licence key scoped to a tenant, a facility or a single deployment.

TENANT

The whole operation.

Every facility and deployment under your account. For a central ERP or BI warehouse.

FACILITY

One site.

One warehouse or plant. A site-level WMS or regional partner reads nothing from other sites.

DEPLOYMENT

One line or department.

A single deployment inside a facility. For a label station, a kiosk or a vendor who should see one line only.

Uniform endpoints

Every service exposes its resources the same way, so an integration written against one service reads like an integration against any other. Each service publishes a Swagger / OpenAPI description of its resources.

VERB	WHAT IT DOES
GET collection	List a resource, paginated
GET by ID	Fetch one record
POST	Create
PUT by ID	Update
DELETE by ID	Delete

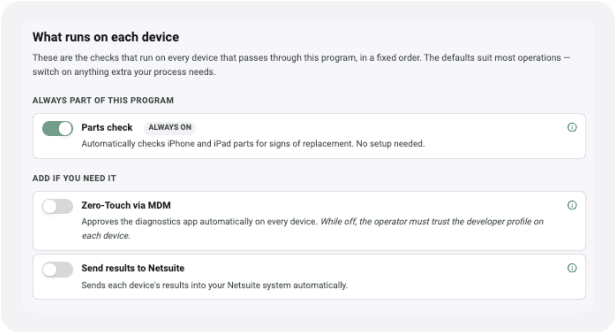


FIG. 9 Control Center → Configuration Wizard → Services & checks. Zero-Touch via MDM and Send results to NetSuite are switched on per program.

A key is a credential. Keep it out of chat, tickets, repositories and logs; if it leaks, Customer Support rotates it. Revoking a key stops every integration that carries it.

INTEGRATION PATTERN	HOW IT IS DONE
ERP and WMS	Switch on Send results to NetSuite per program and each device's results flow into NetSuite. For any other ERP, CRM or WMS, point an automation connection at its endpoint, or pull through REST with a facility-scoped key.
MDM	Zero-Touch via MDM approves the diagnostics app on every device, so no operator trusts a developer profile by hand. MDM enrollment is detected and reported on the record.
Label printing	The Label Printing wizard takes a Reporting export or an uploaded CSV as its data source and maps export columns to label fields, so labels print from the record the API returns.
BI and finance	Scheduled CSV or Excel to a mailbox weekly or monthly, or a tenant-scoped REST pull into the warehouse. The GSMA usage overview exports as CSV for cost allocation.

HONEST SCOPE

The API moves records. It makes no claim the bench did not make first.

It runs no test, erases no drive and issues no certificate. ADISA assurance level 4 applies to Pro-Diagnostics and MacRestore; Pro-Diagnostic PC & Mac reports NIST 800-88 methods with a per-drive erase report. The API returns exactly what those products recorded, with every automated change marked as such, and it never rewrites a device identity.

Connect it to the systems you already run.

Talk to us about API access for your tenant, a key scoped to one site, and a GSMA Device Check key with test mode on from day one. CSV and Excel export are included everywhere.

GET STARTED
onboarding.assetscience.com

PUBLIC CERTIFICATES
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Screenshots are from production builds; device identifiers, operator names, usage figures and customer data shown are synthetic. GSMA is a mark of the GSM Association. Product names and marks belong to their respective owners.