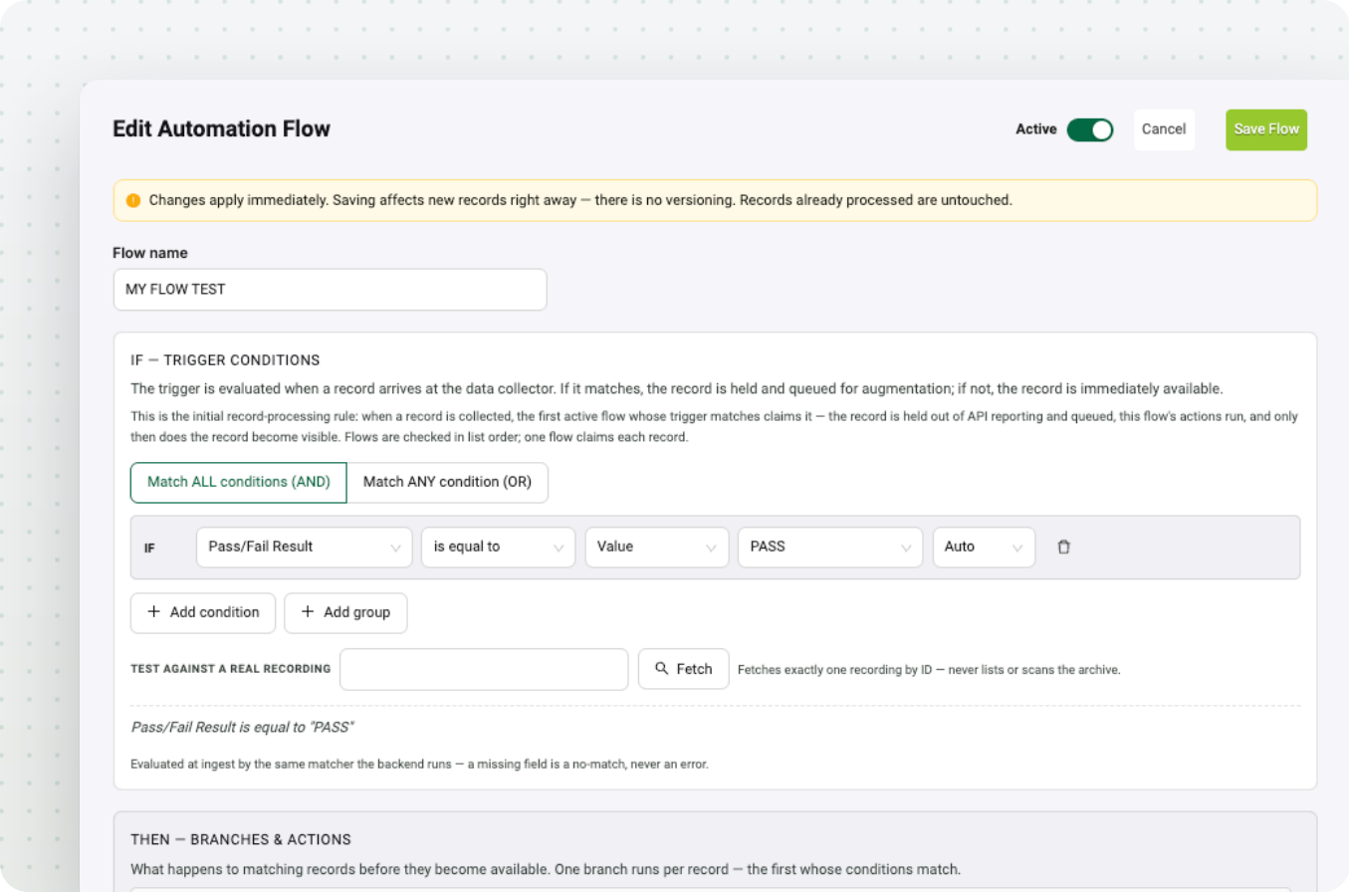
BACK-OFFICE API SUITE

Sus datos, entran y salen, sin pedírnoslo.

Una API REST sobre los servicios de la plataforma, con claves limitadas a un tenant, una sede o un solo despliegue. GSMA Device Check con modo de prueba gratuito. Exportación a CSV y Excel, informes programados a su ritmo y flujos automáticos que cambian un registro o lo envían a sus sistemas antes de que lo vean los informes.



PÚBLICO

Integración, TI y operaciones en procesadores de dispositivos, operadores móviles, aseguradoras e ITAD

INTERFACES

REST · JSON · CSV · Excel · correo programado

WEB

assetscience.com

DE UN VISTAZO

Las ocho preguntas de todo comprador, respondidas para una API.

El Back-Office API Suite mueve registros. No ejecuta pruebas ni borra unidades. Los certificados y la garantía ADISA corresponden a los productos de estación que los producen; la API expone exactamente lo que esos productos registraron.

CERTIFICADO

● No se emite aquí

La API no emite certificados. Devuelve los registros con los que Control Center construye los certificados, incluido el estado de activación, GSMA y restablecimiento de fábrica de cada ejecución. Los certificados son PDF y consulta pública en verified.assetscience.com.

CERTIFICADO ADISA

● No aplicable

No. El nivel de garantía 4 de ADISA se aplica a Pro-Diagnostics y MacRestore, los productos que realizan el borrado. La API transporta sus registros y nunca cambia un resultado de borrado.

TIPO DE BORRADO

● No se realiza

La API no borra nada. Informa del resultado y el método de borrado que registró la estación: borrado de contenido, Express Connect o flasheo desde Pro-Diagnostics, y el informe de borrado NIST 800-88 por unidad de Pro-Diagnostic PC.

PRUEBAS GUIADAS

● No

Sin pantallas de operador. Las pruebas se ejecutan en el puesto de trabajo con los productos de estación; la API mueve sus resultados y permite que sus sistemas reaccionen a ellos.

TIPO DE PRUEBAS

● Ninguna

Expone **cada resultado con sus códigos de fallo** de las 133 pruebas de Android, 83 de iOS, 23 de Mac y 25 de PC, además de resultados de servicios, grado, anulaciones y salud de la batería.

FUNCIONES PRINCIPALES

● 4

Endpoints REST uniformes en los servicios. **Claves** por tenant, sede o despliegue. **GSMA Device Check** con modo prueba gratis. **Exportar a CSV y Excel** con informes programados por email.

PLATAFORMAS

● HTTPS

Cualquier cliente que hable HTTPS y JSON. Tokens Bearer validados contra nuestro proveedor de identidad para personas, claves de licencia para sistemas. Las conexiones de automatización llaman a sus propios endpoints HTTPS.

ANALÍTICA DE DATOS Y API

● Sí

El registro completo del dispositivo: identificadores, dispositivo, sesión, infraestructura, batería, pruebas, servicios, grado y campos propios. **REST**, exportación CSV, Excel y JSON, informes programados por email.

Alcance real. Un "No" en cinco de estas ocho es el objetivo: este producto es la tubería, no el puesto. Si una afirmación sobre un certificado, una norma de borrado o una prueba corresponde a algo, corresponde a Pro-Diagnostics, Pro-Diagnostic PC & Mac o MacRestore, y la hacen sus propios documentos.

QUÉ EXPONE LA API

Un registro por ejecución, con todo lo que el puesto de trabajo puso en él.

Todos los productos de estación escriben el mismo formato de registro en Control Center. La API devuelve ese registro. Su contenido depende de los servicios que el programa ejecutó en el dispositivo.

GRUPO	CAMPOS DEL REGISTRO
Identificadores	IMEI, IMEI 2, MEID, serie, GUID, ECID, ICCID, MAC Wi-Fi y Bluetooth
Dispositivo	Fabricante, nombre y número de modelo, tipo de producto, versión de OS, almacenamiento, color, región, categoría
Sesión	ID de sesión, ID entre sistemas, nombre del proceso, flujo y ruta, inicio, fin, duración, turno, equipo, operador
Infraestructura	Sede, despliegue, nombre del equipo, compilación del software de escritorio
Batería	Nivel, temperatura, estado de carga, ciclos, salud, capacidad máxima
Resultado	Correcto, fallo o incompleto; cada prueba con códigos de fallo; servicios ejecutados; grado; anulaciones
Campos propios	Sus propias claves, definidas en Control Center o escritas por un flujo

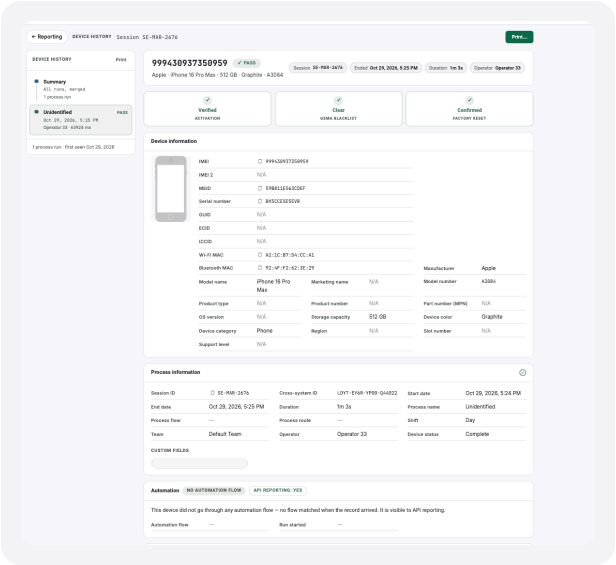


FIG. 1 Control Center → Reporting → Device History. Cabecera del registro con su estado de activación, GSMA y restablecimiento de fábrica, el bloque de identificadores y la información del proceso. Identificadores sintéticos.

RESULTADOS Y GRADOS

Lo que decidió el puesto.

El resultado de la ejecución es PASS, FAIL o INCOMPLETE, nunca un booleano simple. Cada prueba lleva su resultado y sus códigos de fallo, con el más significativo en un campo dedicado de motivo de fallo. Activación, GSMA, restablecimiento de fábrica y comprobación de piezas van en el mismo registro; los registros de clasificación llevan el grado como cadena de categoría propia.

BORRADO: INFORMES Y CERTIFICADOS

La estación los registra; usted los lee.

El resultado y el método de borrado proceden del producto que hizo el trabajo: borrado de contenido o flasheo en Pro-Diagnostics, un informe de borrado NIST 800-88 por unidad en Pro-Diagnostic PC. Los certificados se generan desde estos registros en Control Center y se publican en verified.assetscience.com; la API lee el registro subyacente.

PROCEDENCIA

Un valor automático nunca pasa por dato del puesto.

Cada campo que cambia un flujo se anota en el registro con el nombre del flujo, la hora, el valor original y el nuevo, y se ve en Device History. La identidad del dispositivo, los ID de sesión y la identidad del operador nunca los puede escribir un flujo.

ENTRADA Y SALIDA

Los registros llegan del puesto, de un archivo o de su sistema. Salen con el formato que necesite.

Entrada de datos. La mayoría de los registros llegan solos desde las estaciones. Existen tres rutas más para todo lo demás.

- **Identificadores.** Cada programa declara los identificadores mínimos que debe llevar un registro, como el número de serie del OEM, y los campos obligatorios antes de aceptar una ejecución.
- **Campos propios.** Defina sus propias claves en Control Center como campos de lista, numéricos o de texto, mostrados al iniciar sesión el operador o al final del proceso, con nombres visibles por idioma. Viajan en cada registro y cada exportación.
- **Data Import Tool.** Suba una lista de dispositivos desde la plantilla CSV contra una sede, despliegue, turno, equipo y programa, con validación del archivo antes de importar, o introduzca un dispositivo a mano.
- **REST.** Los mismos endpoints de recursos que leen registros también los crean y actualizan, de modo que un sistema de terceros puede enviar datos además de extraerlos.

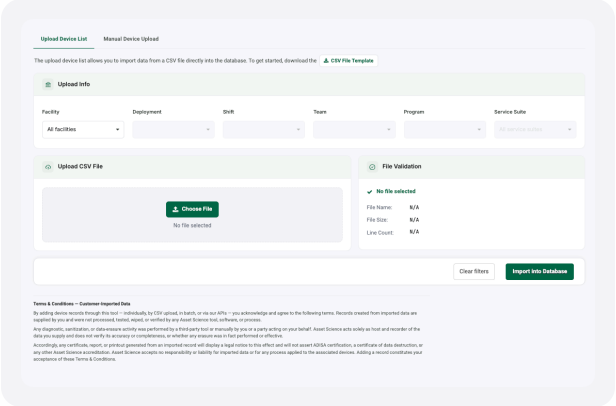


FIG. 2 Control Center → Data Import Tool → Upload Device List. Plantilla CSV, sede y programa de destino, validación del archivo y el aviso que llevan los registros importados.

Un registro importado se marca como tal. Un registro creado desde un archivo o a través de la API no fue procesado por una herramienta de Asset Science. Cualquier certificado o impresión generada a partir de él lleva un aviso legal en ese sentido y no afirma ninguna certificación ADISA ni ningún certificado de destrucción de datos.

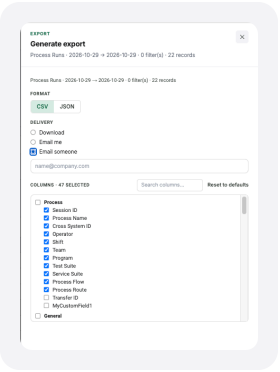


FIG. 3 Reporting → Generate export. CSV o JSON, descarga o correo, 47 columnas elegidas del registro.

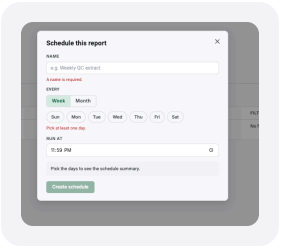


FIG. 4 Reporting → Schedule this report. Semanal o mensual, los días y la hora del día.

Salida de datos. El registro es suyo, en cinco formatos.

- **REST.** Liste con paginación u obtenga un registro por su ID, filtrado al tenant, la sede o el despliegue al que la clave está limitada.
- **CSV y Excel.** Cualquier vista de Reporting, con las columnas que elija, descargada o enviada por correo a usted o a otra persona.
- **JSON.** La misma exportación en JSON para un sistema que prefiera analizar en vez de importar.
- **Informes periódicos.** Nombre un informe, elija semanal o mensual, marque los días y la hora de ejecución; llega por correo con esa cadencia.
- **Exportaciones.** Cada exportación generada se lista con su número de registros y su tamaño, lista para descargar de nuevo o alimentar la impresora de etiquetas.

FLUJOS AUTOMÁTICOS

Si este registro, ENTONCES cámbielo o envíelo, antes de que lo vean los informes.

Los flujos son reglas que escriben sus propios administradores en Control Center, ordenadas como reglas de correo. El primer flujo cuyo disparador coincide reclama el registro, ejecuta sus acciones y solo entonces lo libera a los informes y a la API.

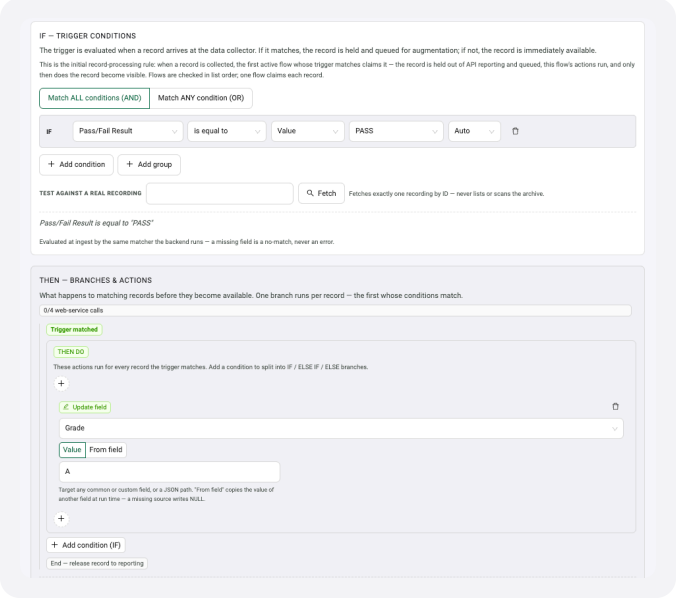


FIG. 5 Control Center → Automation → Edit Automation Flow. IF: Pass/Fail Result is equal to PASS, probado contra una grabación real. THEN: Update field Grade = A.

IF. Las condiciones son campo, operador y valor: es igual a, no es igual a, contiene, es mayor o menor que, es nulo, no es nulo. Combínelas con AND u OR, con un nivel de agrupación. Elija de un catálogo de campos comunes, de sus campos propios o de cualquier ruta JSON del registro. Antes de guardar, obtenga una grabación real por ID de registro o IMEI y vea si coincide.

THEN. Una cadena de IF, ELSE IF y ELSE; se ejecuta exactamente una rama por registro. Tres acciones: **Editar campo** con un valor escrito o copiado de otro campo, **Llamar web-service**, y **Fin**. Lo guardado llega a los nuevos registros en un minuto.

Si el flujo falla. Los errores transitorios se reintentan con espera progresiva. Un fallo permanente sigue la política del flujo: liberar el registro sin ampliar y marcado, o bloquearlo hasta que una persona lo libere. Nada se pierde y un registro nunca se muestra a medio cambiar.

Conexiones son las llamadas a web-service reutilizables que puede hacer un flujo: su propio endpoint HTTPS, el método y una cabecera Bearer, API-key o Basic con un secreto de solo escritura, enmascarado tras guardar y omitido en los logs.

- **Payload a elección.** Campos propios más el ID del registro por defecto, o el registro completo. Las credenciales y la identidad del operador siempre se eliminan.
- **Respuesta devuelta.** Las claves de la respuesta JSON aterrizan en campos propios, de modo que una consulta al ERP puede enriquecer el registro.
- **Validar antes.** Una llamada de muestra muestra la respuesta del servidor en línea; no se escribe nada en ningún registro.
- **Acotado.** Como máximo cuatro llamadas por flujo. Todo el flujo se reejecuta al reintentar, así que su endpoint debe ser idempotente.

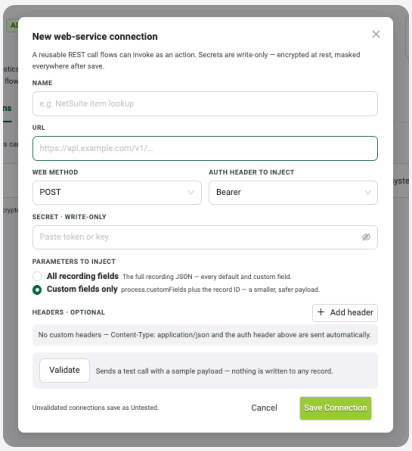


FIG. 6 Automation → Connections → New web-service connection: URL, método, cabecera de autenticación, secreto de solo escritura, alcance del payload, Validate.

GSMA DEVICE CHECK

Consultas de perdidos y robados, con modo de prueba gratuito antes de decidir.

Cada comprobación busca un IMEI, MEID o ESN en el registro GSMA de dispositivos perdidos y robados y devuelve su historial de bloqueo. Ejecútela desde el puesto con Pro-Diagnostics o llámela desde su propio sistema con una clave de licencia.

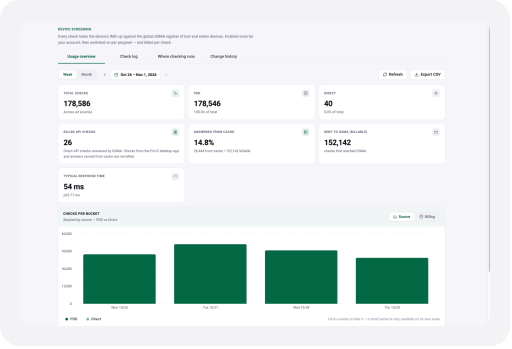


FIG. 7 Control Center → GSMA Blacklist → Usage overview. Comprobaciones por origen, cuántas se respondieron desde caché, cuántas llegaron a GSMA y el tiempo de respuesta típico. Datos de demostración.

```
GET /api/gsma/blacklist?imei=9994309373509 59&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"
}
```

Abreviado. Se indica exactamente uno de imei, meid o esn. El estado de blocklist y greylist es Yes o No; el historial está vacío para un dispositivo limpio.

Prueba gratuita. Con el modo de prueba activado, la llamada devuelve un payload de muestra fijo, nunca llega a GSMA y nunca se factura. Una sola llamada de extremo a extremo confirma su clave, su ruta de red y su analizador antes de cualquier tráfico de producción.

Caché, no factura. Un dispositivo ya consultado dentro de la ventana de caché se responde desde caché y no se factura; solo un dispositivo nuevo se envía a GSMA. La pantalla de uso muestra el reparto, de modo que la economía unitaria es visible en vez de deducirse de una factura.

Errores claros. Un identificador ausente o mal formado es un 400, una clave incorrecta un 403, un fallo de GSMA aguas arriba un 500 que se puede reintentar una vez con seguridad.

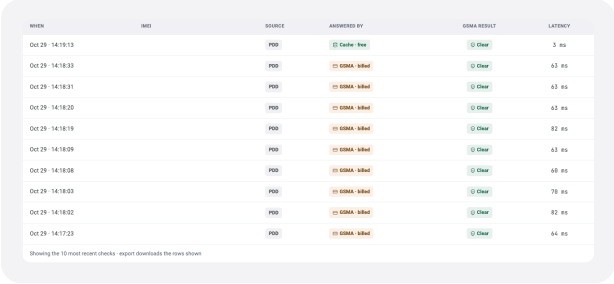


FIG. 8 GSMA Blacklist → Check log. Una fila por comprobación: origen, respondida desde caché o por GSMA, resultado y latencia. Columna IMEI en blanco; exportable como CSV.

Bloqueos: se informan, nunca se eliminan. Un dispositivo en lista de bloqueo se registra como bloqueado y se enruta según su flujo de trabajo. La comprobación indica el estado del dispositivo en GSMA; no hace nada al dispositivo.

CLAVES, ALCANCE Y PATRONES DE INTEGRACIÓN

Cada clave alcanza solo la parte de la operación para la que se emitió.

Las personas inician sesión con un token Bearer validado por nuestro proveedor de identidad. Los sistemas usan una clave de licencia limitada a un tenant, una sede o un solo despliegue.

TENANT

Toda la operación.

Todas las sedes y despliegues de su cuenta. Para un ERP central o un almacén de BI.

SEDE

Un sitio.

Un almacén o planta. Un WMS de sede o un socio regional no lee nada de otras sedes.

DESPLIEGUE

Una línea o departamento.

Un solo despliegue en una sede. Para una estación de etiquetado, un quiosco o un proveedor que solo vea una línea.

Endpoints uniformes

Cada servicio expone sus recursos igual, así una integración escrita contra un servicio se lee como una contra cualquier otro. Cada servicio publica una descripción Swagger / OpenAPI de sus recursos.

MÉTODO	QUÉ HACE
GET colección	Lista un recurso, paginado
GET por ID	Lee un registro
POST	Crea
PUT por ID	Edita
DELETE por ID	Elimina

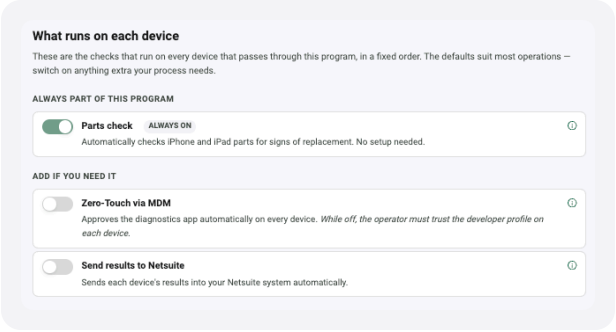


FIG. 9 Control Center → Configuration Wizard → Services & checks. Zero-Touch vía MDM y Send results to NetSuite se activan por programa.

Una clave es credencial. Manténgala fuera del chat, los tickets, los repositorios y los logs; si se filtra, el Soporte al Cliente la rota. Revocar una clave detiene toda integración que la use.

PATRÓN DE INTEGRACIÓN	CÓMO SE HACE
ERP y WMS	Active Send results to NetSuite por programa y los resultados de cada dispositivo fluyen a NetSuite. Para otro ERP, CRM o WMS, apunte una conexión de automatización a su endpoint, o extraiga por REST con una clave limitada a la sede.
MDM	Zero-Touch vía MDM aprueba la app de diagnóstico en cada dispositivo, así ningún operador confía a mano en un perfil de desarrollador. La inscripción en MDM se detecta y consta en el registro.
Etiquetas	El asistente de Label Printing usa una exportación de Reporting o un CSV subido como fuente y asigna columnas de exportación a campos de etiqueta: las etiquetas salen del registro que devuelve la API.
BI y finanzas	CSV o Excel programado a un buzón, semanal o mensual, o extracción REST limitada al tenant al almacén. La vista de uso de GSMA sale en CSV para asignar costes.

ALCANCE REAL

La API mueve registros. No afirma nada que el puesto no afirmara antes.

No ejecuta pruebas, no borra unidades y no emite certificados. El nivel de garantía 4 de ADISA se aplica a Pro-Diagnostics y MacRestore; Pro-Diagnostic PC & Mac informa de métodos NIST 800-88 con un informe de borrado por unidad. La API devuelve exactamente lo que esos productos registraron, con cada cambio automático marcado como tal, y nunca reescribe la identidad de un dispositivo.

Conéctela a los sistemas que ya utiliza.

Hable con nosotros sobre el acceso a la API para su tenant, una clave limitada a una sede y una clave de GSMA Device Check con modo de prueba activado desde el primer día. La exportación a CSV y Excel está incluida en todas partes.

EMPEZAR
onboarding.assetscience.com

CERTIFICADOS PÚBLICOS
verified.assetscience.com/verify

WEB
assetscience.com

© 2026 Asset Science. Las capturas proceden de compilaciones de producción; los identificadores de dispositivo, nombres de operador, cifras de uso y datos de cliente mostrados son sintéticos. GSMA es una marca de la GSM Association. Los nombres y marcas de productos pertenecen a sus respectivos propietarios.