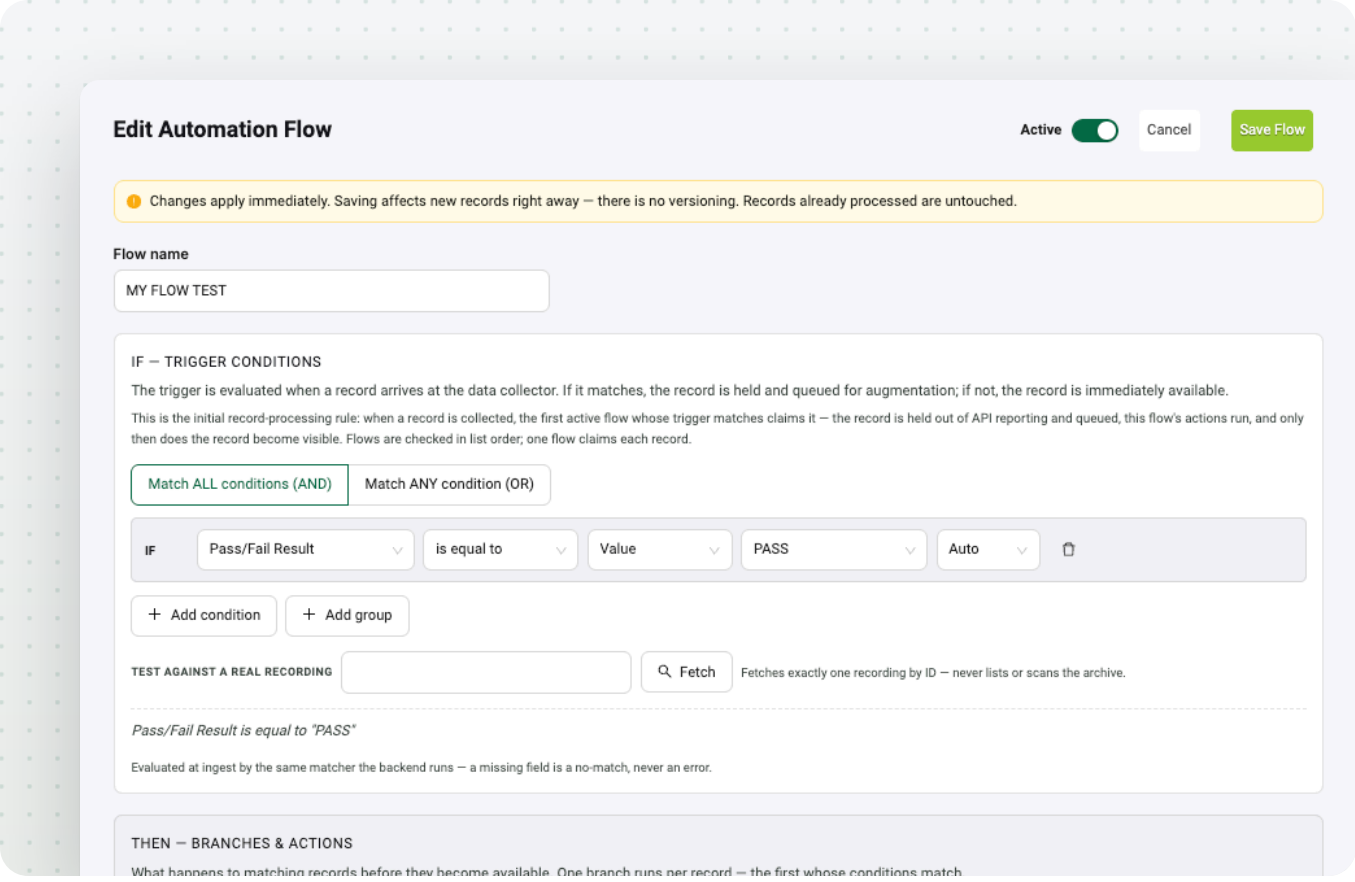
BACK-OFFICE API SUITE

データの入出力を、当社に頼らず自社で。

プラットフォームの各サービスを横断する REST API。キーはテナント、拠点、または単一デプロイメント単位でスコープを設定できます。無料テストモード付きの GSMA Device Check。CSV・Excel エクスポート、任意の頻度での定期レポート、そしてレポートに現れる前にレコードを変更したり自社システムへ送信したりする自動化フロー。



対象読者
デバイス処理事業者、通信事業者、保険会社、ITAD 事業者の統合・IT・運用責任者

インターフェース
REST · JSON · CSV · Excel · 定期メール配信

ウェブ
assetscience.com

概要一覧

購入検討者が必ず尋ねる 8 つの質問に、API の視点で回答します。

Back-Office API Suite はレコードを動かす製品です。テストは実行せず、ドライブも消去しません。証明書と ADISA 保証は、それらを生成するステーション製品に属します。API は、それらの製品が記録した内容をそのまま公開します。

証明書

● 本製品では発行しません

API は証明書を発行しません。 Control Center が証明書を生成する元となるレコードを返します。各実行のアクティベーション、GSMA、工場出荷時リセットの状態も含まれます。証明書そのものは PDF と verified.assetscience.com での公開照会で提供されます。

ADISA 認証

● 該当なし

いいえ。 ADISA 保証レベル 4 は、消去を実行する製品である Pro-Diagnostics と MacRestore に適用されます。API はそれらのレコードを運ぶだけで、消去結果を変更することはありません。

消去の種類

● 実行しません

API は何も消去しません。ステーションが記録した消去結果と方式を報告します。Pro-Diagnostics によるコンテンツ消去、Express Connect、フラッシュ、および Pro-Diagnostic PC によるドライブ単位の NIST 800-88 消去レポートです。

ガイド付きユーザーテスト

● いいえ

オペレーター画面はありません。テストは作業台でステーション製品が実行します。API はその結果を運び、自社システムが結果に応じて動作できるようにします。

テストの種類

● 実行しません

公開対象： **すべてのテスト結果と失敗コード** 。Android 133、iOS 83、Mac 23、PC 25 の各テストに加え、サービス結果、グレード、上書き、バッテリー健全性も含みます。

主な機能

● 4

統一された REST エンドポイント を各サービスで提供。 **スコープ付きキー** ：テナント、拠点、デプロイメント単位。 **GSMA Device Check** ：無料テストモード付き。 **CSV・Excel エクスポート** ：定期レポートをメール配信。

対応プラットフォーム

● HTTPS

HTTPS と JSON を扱えるすべてのクライアント。人にはアイデンティティプロバイダーで検証される Bearer トークン、システムにはライセンスキーを使用します。自動化接続は自社の HTTPS エンドポイントを呼び出します。

データ分析と API

● はい

完全なデバイスレコード：識別子、デバイス、セッション、インフラ、バッテリー、テスト、サービス、グレード、カスタムフィールド。 **REST**、CSV・Excel・JSON エクスポート、メールによる定期レポート。

正直な範囲。 8 項目のうち 5 項目が「いいえ」であることこそが要点です。本製品は配管であり、作業台ではありません。証明書、消去規格、テストに関する主張は、Pro-Diagnostics、Pro-Diagnostic PC & Mac、MacRestore に属するものであり、それぞれのホワイトペーパーで述べられています。

API が公開する内容

処理実行ごとに 1 件のレコード。作業台が入力したすべてを保持します。

すべてのステーション製品が、同じ形式のレコードを Control Center に書き込みます。API はそのレコードを返します。内容は、そのデバイスでプログラムが実行したサービスによって決まります。

グループ	レコード上のフィールド
識別子	IMEI、IMEI 2、MEID、シリアル、GUID、ECID、ICCID、Wi-Fi MAC、Bluetooth MAC
デバイス	メーカー、モデル名・型番、製品タイプ、OS バージョン、ストレージ、色、地域、カテゴリー
セッション	セッション ID、システム間 ID、プロセス名、フローとルート、開始、終了、所要時間、シフト、チーム、オペレーター
インフラ	拠点、デプロイメント、コンピューター名、デスクトップソフトウェアのビルド
バッテリー	残量、温度、充電状態、サイクル数、健全性、最大容量
結果	合格・不合格・未完了、失敗コード付きの全テスト、実行したサービス、グレード、上書き
カスタムフィールド	Control Center で定義した独自のキー、またはフローが書き込んだ値

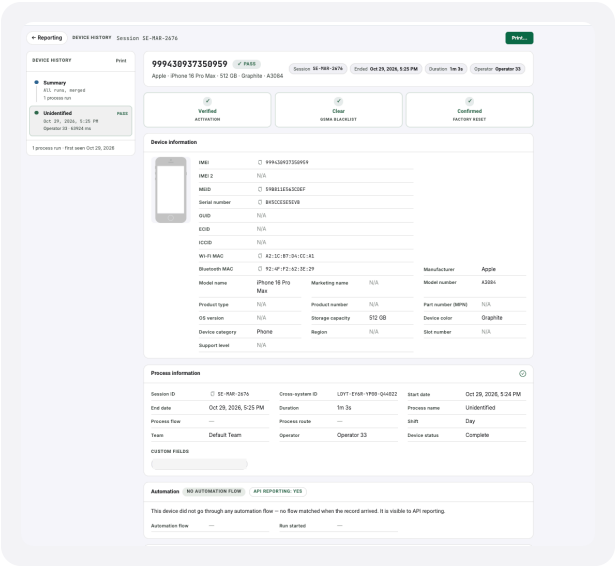


図1 Control Center → Reporting → Device History。アクティベーション、GSMA、工場出荷時リセットの状態を含むレコードヘッダー、識別子ブロック、プロセス情報。識別子は架空のものです。

結果とグレード

作業台が下した判定。

実行結果は PASS、FAIL、INCOMPLETE のいずれかであり、単なる真偽値ではありません。各テストは独自の結果と失敗コードを持ち、最も重要なコードは専用の失敗理由フィールドに入ります。アクティベーション、GSMA、工場出荷時リセット、パーツチェックも同じレコード上にあります。グレーディングのレコードは、グレードを自社のカテゴリー文字列として保持します。

消去レポートと証明書

ステーションが記録し、お客様が読み取ります。

消去結果と方式は、実際に作業を行った製品から得られます。Pro-Diagnostics のコンテンツ消去またはフラッシュ、Pro-Diagnostic PC のドライブ単位の NIST 800-88 消去レポートです。証明書はこれらのレコードから Control Center で生成され、verified.assetscience.com で公開されます。API はその背後にあるレコードを読み取ります。

来歴

自動生成された値が作業台のデータになりすますことはありません。

フローが変更したすべてのフィールドは、フロー名、時刻、変更前の値、変更後の値とともにレコードに記録され、Device History に表示されます。デバイス識別情報、セッション ID、オペレーター識別情報をフローが書き込むことはできません。

データの入力と出力

レコードは作業台から、ファイルから、または自社システムから届きます。出力は必要な形式で行えます。

データを入れる。 ほとんどのレコードはステーションから自動的に届きます。それ以外については 3 つの経路があります。

- **識別子。** 各プログラムは、レコードが保持すべき最小限の識別子（OEM シリアル番号など）と、実行を受け付ける前に必須となるフィールドを宣言します。
- **カスタムフィールド。** Control Center でリスト型、数値型、文字列型の独自キーを定義し、オペレーターのログイン時またはプロセス終了時に表示できます。表示名は言語ごとに設定できます。これらはすべてのレコードとエクスポートに付随します。
- **Data Import Tool。** CSV テンプレートからデバイスリストを拠点、デプロイメント、シフト、チーム、プログラムに対してアップロードできます。インポート前にファイル検証が行われます。1 台ずつ手入力することも可能です。
- **REST.** レコードを読み取るのと同じリソースエンドポイントで作成・更新も行えるため、サードパーティシステムはデータの取得だけでなく投入も可能です。

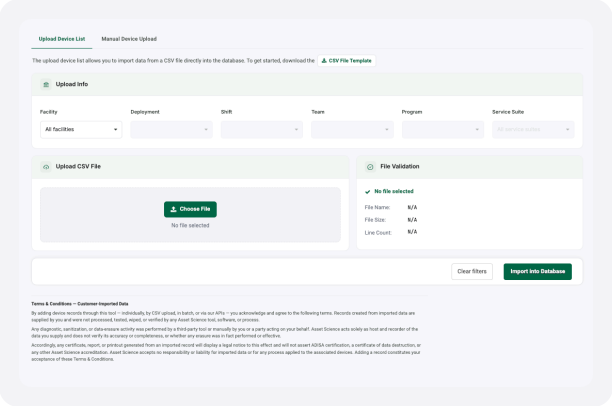


図2 Control Center → Data Import Tool → Upload Device List。CSV テンプレート、対象の拠点とプログラム、ファイル検証、およびインポートされたレコードに付く注意書き。

インポートされたレコードにはインポート済みの印が付きます。 ファイルまたは API から作成されたレコードは、Asset Science のツールで処理されたものではありません。そこから生成される証明書や印刷物には、その旨の法的注意書きが付き、ADISA 認証もデータ破壊証明も主張しません。

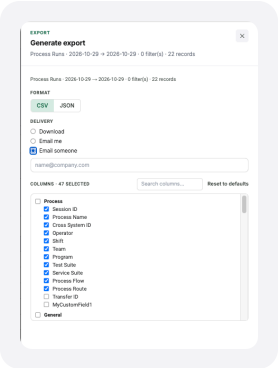


図3 Reporting → Generate export。CSV または JSON、ダウンロードまたはメール送信、レコードから選んだ 47 列。

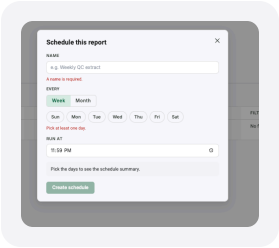


図4 Reporting → Schedule this report。週次または月次、曜日と時刻を指定。

データを出す。 レコードはお客様のものです。5 つの形式で提供します。

- **REST.** ページネーション付きの一覧取得、または ID による単一レコードの取得。キーのスコープであるテナント、拠点、デプロイメントに絞り込まれます。
- **CSV と Excel。** 任意の Reporting ビューを、選んだ列で、ダウンロードまたは自分や他者へのメール送信。
- **JSON.** インポートよりも解析を好むシステム向けに、同じエクスポートを JSON で提供。
- **定期レポート。** レポートに名前を付け、週次か月次を選び、曜日と実行時刻を指定します。その頻度でメールが届きます。
- **エクスポート履歴。** 生成されたすべてのエクスポートがレコード件数とサイズとともに一覧表示され、再ダウンロードやラベルプリンターへの投入が可能です。

自動化フロー

IF このレコードなら、THEN 変更するか送信する。レポートに現れる前に。

フローは自社の管理者が Control Center で作成するルールで、メールルールのように順序付けます。トリガーが最初に一致したフローがレコードを占有してアクションを実行し、その後にのみレポートと API へ解放します。

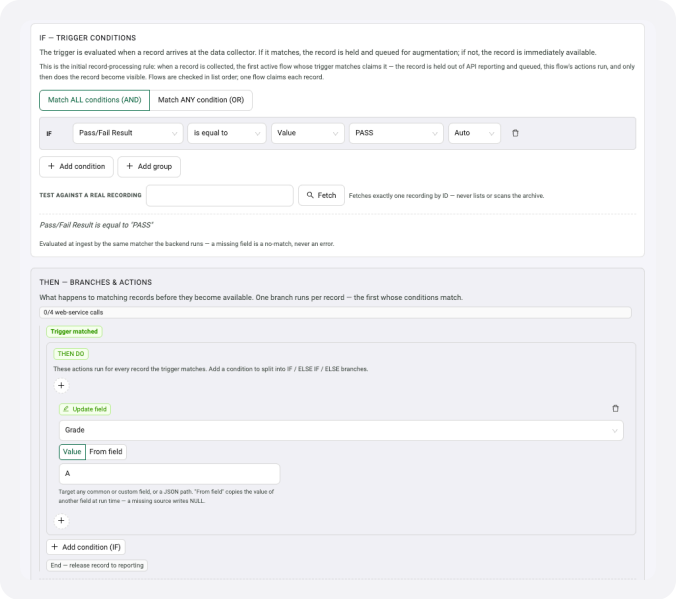


図5 Control Center → Automation → Edit Automation Flow。IF：Pass/Fail Result is equal to PASS を実際の記録に対して検証。THEN：Update field で Grade = A。

IF. 条件はフィールド・演算子・値で構成します（is equal to、is not equal to、contains、is greater or smaller than、is null、is not null）。AND/OR で組み合わせ、グループ化は 1 階層まで。一般的なフィールドのカタログ、カスタムフィールド、レコード内の任意の JSON パスから選べます。保存前に、レコード ID か IMEI で実際の記録を 1 件取得し、一致を確認できます。

THEN. IF、ELSE IF、ELSE の連鎖。レコードごとに実行される分岐は必ず 1 つです。アクションは 3 種類： **Update field** （入力した値、または他フィールドからコピーした値を設定）、 **Call web-service**、および **終了**。保存した変更は約 1 分以内に新規レコードへ反映されます。

フローが失敗した場合。 一時的なエラーはバックオフ付きで再試行します。恒久的な失敗はフローのポリシーに従い、レコードを未補強のままフラグ付きで解放するか、担当者が解放するまでブロックします。何も失われず、変更途中のレコードが表示されることもありません。

接続 はフローが呼び出す再利用可能な Web サービス呼び出しです。自社の HTTPS エンドポイント、メソッド、Bearer・API キー・Basic ヘッダーと書き込み専用シークレットを設定します。シークレットは保存後にマスクされ、ログからも除去されます。

- **ペイロードは選択可能。** 既定はカスタムフィールドとレコード ID、または完全なレコード。認証情報と操作者情報は常に除去します。
- **レスポンスの書き戻し。** JSON 応答のキーがカスタムフィールドに入り、ERP 照会でレコードを補強できます。
- **まず検証。** サンプル呼び出しで応答をその場で確認でき、レコードには書き込まれません。
- **上限あり。** 1 フローあたり最大 4 回。再試行はフロー全体を再実行するため、エンドポイントは冪等にしてください。

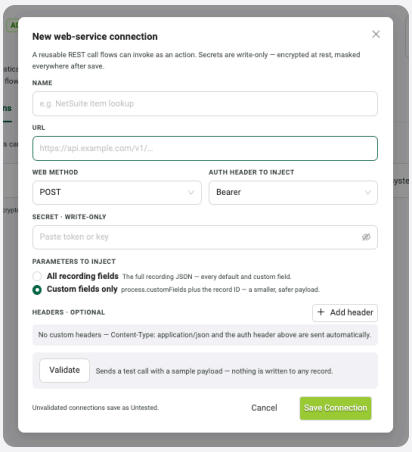


図6 Automation → Connections → New web-service connection：URL、メソッド、認証、Validate。

GSMA DEVICE CHECK

紛失・盗難チェック。導入前に試せる無料テストモード付き。

各チェックは IMEI、MEID、ESN を GSMA の紛失・盗難デバイス登録と照合し、ブロックリスト履歴を返します。Pro-Diagnostics から作業台で実行することも、ライセンスキーで自社システムから呼び出すこともできます。

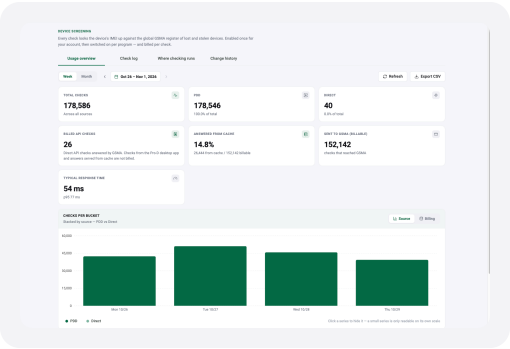


図7 Control Center → GSMA Blacklist → Usage overview。ソース別のチェック数、キャッシュから応答した件数、GSMA に到達した件数、標準的な応答時間。デモデータです。

```
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",
  "blacklistst atus": "Yes",
  "greylistst atus": "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"
}
```

抜粋。imei、meid、esn のいずれか 1 つだけを指定します。ブロックリストとグレーリストの状態は Yes または No で、クリーンなデバイスでは履歴は空になります。

無料テストモード。 テストモードを有効にすると、呼び出しは固定のサンプルペイロードを返し、GSMA には到達せず、課金もされません。この呼び出しを一度エンドツーエンドで行えば、本番トラフィックの前にキー、ネットワーク経路、パーサーを確認できます。

キャッシュであり、請求ではありません。 キャッシュ期間内に照会済みのデバイスはキャッシュから応答され、課金されません。GSMA に送られるのは初回のデバイスのみです。使用状況画面にその内訳が表示されるため、単位あたりの収支を請求書から推測せずに把握できます。

明快なエラー。 識別子の欠落や不正は 400、キーの不備は 403、上流の GSMA 障害は 1 回の再試行が安全な 500 を返します。

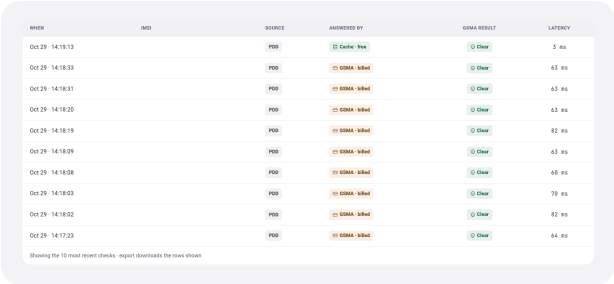


図8 GSMA Blacklist → Check log。チェックごとに 1 行：ソース、キャッシュか GSMA か、結果、レイテンシ。IMEI 列は伏せてあり、CSV でエクスポートできます。

ロックは報告するのみで、解除は行いません。 ブロックリスト登録済みのデバイスはその旨が記録され、お客様のワークフローに従って振り分けられます。チェックはデバイスの GSMA における状態を知らせるだけで、デバイスには何もしません。

キー、スコープ、統合パターン

キーは、発行された範囲の業務にのみ到達します。

人はアイデンティティプロバイダーで検証される Bearer トークンでサインインします。システムは、テナント、拠点、または単一デプロイメントにスコープされたライセンスキーを使用します。

テナント

業務全体。

アカウント配下のすべての拠点とデプロイメント。中央の ERP や BI ウェアハウス向け。

拠点

1 サイト。

1 つの倉庫または工場。サイト単位の WMS や地域パートナーは、他サイトのデータを一切読み取れません。

デプロイメント

1 ラインまたは 1 部門。

拠点内の単一デプロイメント。ラベルステーション、キオスク、または 1 ラインのみを見るべきベンダー向け。

統一されたエンドポイント

すべてのサービスが同じ方法でリソースを公開するため、あるサービス向けに書いた統合は、他のどのサービス向けの統合とも同じように読めます。各サービスはリソースの Swagger / OpenAPI 記述を公開します。

メソッド	機能
GET コレクション	リソースを一覧取得（ページネーション付き）
GET（ID 指定）	レコードを 1 件取得
POST	作成
PUT（ID 指定）	更新
DELETE（ID 指定）	削除

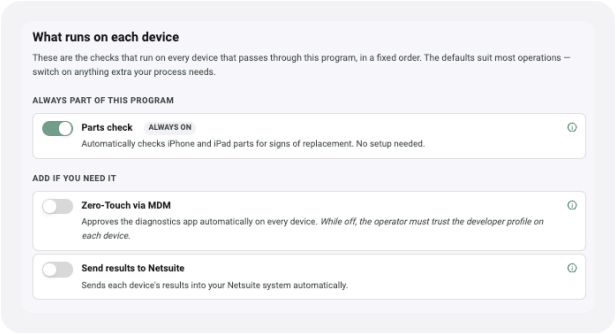


図9 Control Center → Configuration Wizard → Services & checks。Zero-Touch via MDM と Send results to NetSuite はプログラムごとに有効化します。

キーは認証情報です。 チャット、チケット、リポジトリ、ログに残さないでください。漏洩した場合はカスタマーサポートがローテーションします。キーを失効させると、そのキーを使うすべての統合が停止します。

統合パターン	実現方法
ERP と WMS	プログラムごとに Send results to NetSuite を有効にすると、各デバイスの結果が NetSuite に流れます。その他の ERP、CRM、WMS には、自動化接続をそのエンドポイントに向けるか、拠点スコープのキーで REST から取得します。
MDM	Zero-Touch via MDM が各デバイスで診断アプリを承認するため、オペレーターが開発者プロファイルを手動で信頼する必要はありません。MDM への登録は検出され、レコードに記録されます。
ラベル印刷	Label Printing ウィザードは、Reporting のエクスポートまたはアップロードした CSV をデータソースとして取り込み、エクスポート列をラベルのフィールドにマッピングします。つまり、API が返すレコードからラベルが印刷されます。
BI と財務	週次または月次で CSV・Excel をメールボックスへ配信するか、テナントスコープの REST でウェアハウスに取り込みます。GSMA の使用状況概要は、コスト配賦用に CSV でエクスポートできます。

正直な範囲

API はレコードを動かします。作業台が先に述べていない主張は一切しません。

テストは実行せず、ドライブも消去せず、証明書も発行しません。ADISA 保証レベル 4 は Pro-Diagnostics と MacRestore に適用されます。Pro-Diagnostic PC & Mac は、ドライブ単位の消去レポートとともに NIST 800-88 の方式を報告します。API はそれらの製品が記録した内容をそのまま返し、自動変更はすべてその旨を明示します。デバイス識別情報を書き換えることは決してありません。

すでに運用しているシステムに接続しましょう。

テナント向けの API アクセス、1 サイトにスコープしたキー、初日からテストモードを有効にした GSMA Device Check キーについてご相談ください。CSV・Excel エクスポートはすべてに含まれます。

導入の進め方
onboarding.assetscience.com

公開証明書
verified.assetscience.com/verify

ウェブ
assetscience.com

© 2026 Asset Science. スクリーンショットは製品ビルドのものです。表示されているデバイス識別子、オペレーター名、使用状況の数値、顧客データは架空のものです。GSMA は GSM Association のマークです。製品名およびマークは各所有者に帰属します。