

PRODUCT AUTHENTICATION PLATFORM

Features & User Guide

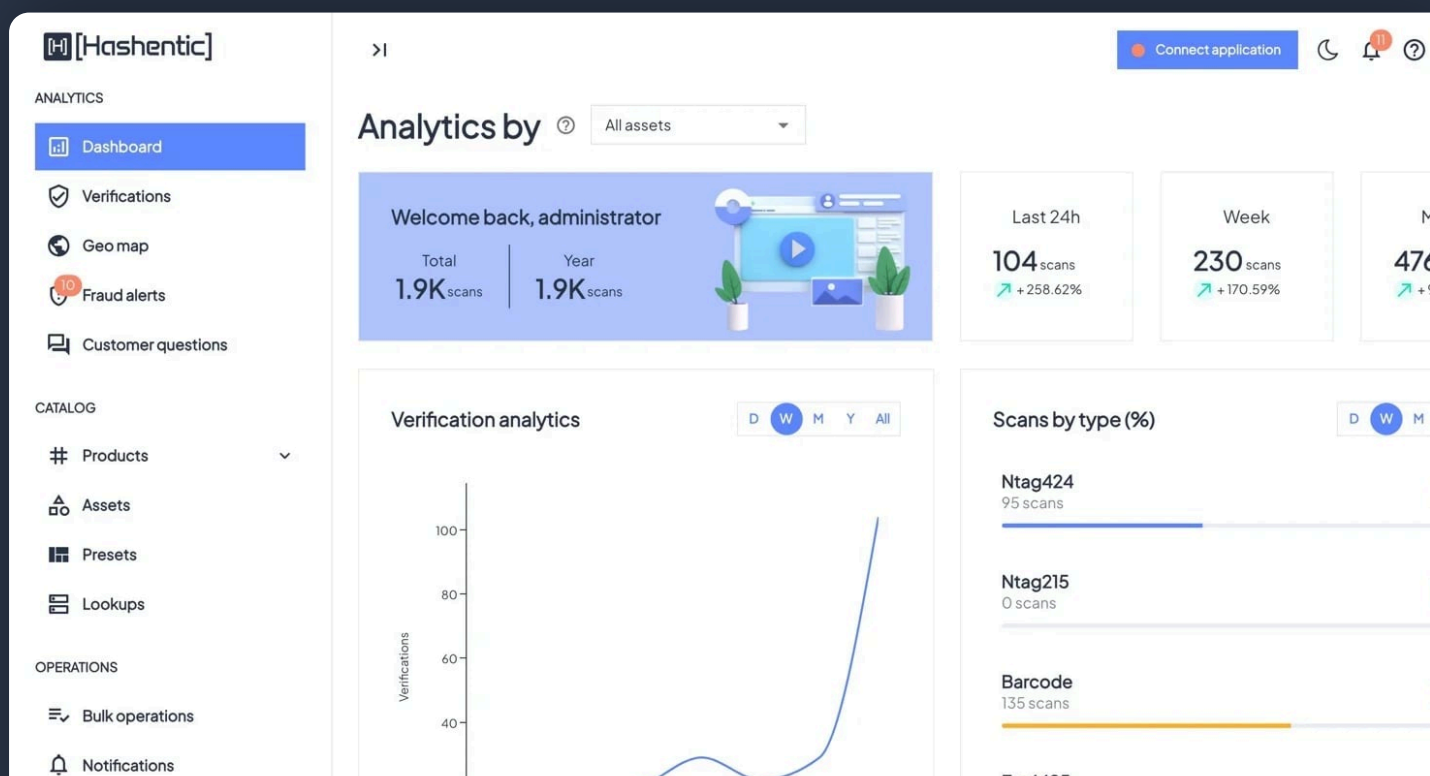
Everything Hashentic can do for your brand, and how to do it:
from tagging your first product to answering a counterfeit alert.

Admin panel

Verification page

Mobile app

Desktop utility



What's inside

Part I Overview	4
1 Hashentic at a glance	5
2 Key concepts	6
3 Roles, permissions and your license	7
4 Finding your way around	9
Part II Feature catalog	11
5 Dashboard	12
6 Verifications	13
7 Geo map	15
8 Fraud & anomaly alerts	16
9 Customer questions	18
10 Products	19
11 Assets and fields	22
12 Verification page templates	25
13 Presets and lookups	29
14 Labels and forms	31
15 Workflows	33
16 Writing tags and printing barcodes	35
17 Bulk operations and ERP	38
18 Notifications and audit log	40
19 AI features	42
20 Users and access	44
21 Settings, branding and license	45
22 Mobile app and Desktop utility	48
23 The consumer verification page	50
Part III Step-by-step guides	52
24 Secure your account	53
25 Set up a new product line	53

26	Design the verification page	54
27	Translate the verification page	56
28	Show a different page when a scan fails	57
29	Create QR-coded products and print labels	57
30	Write NFC tags with the Desktop utility	59
31	Investigate a fraud alert	59
32	Block cloned tags automatically	60
33	Collect warranty registrations	61
34	Add a team member	61
35	Update many products at once	62
36	Help the AI answer your customers	62
37	Connect the mobile app	63

Appendix Reference 64

A	Verification failure reasons	65
B	Template placeholders	66
C	Languages, formats and limits	66
D	Troubleshooting and FAQ	67



Overview

What Hashentic is, the handful of ideas everything else is built on, and how to find your way around the admin panel.

01 Hashentic at a glance

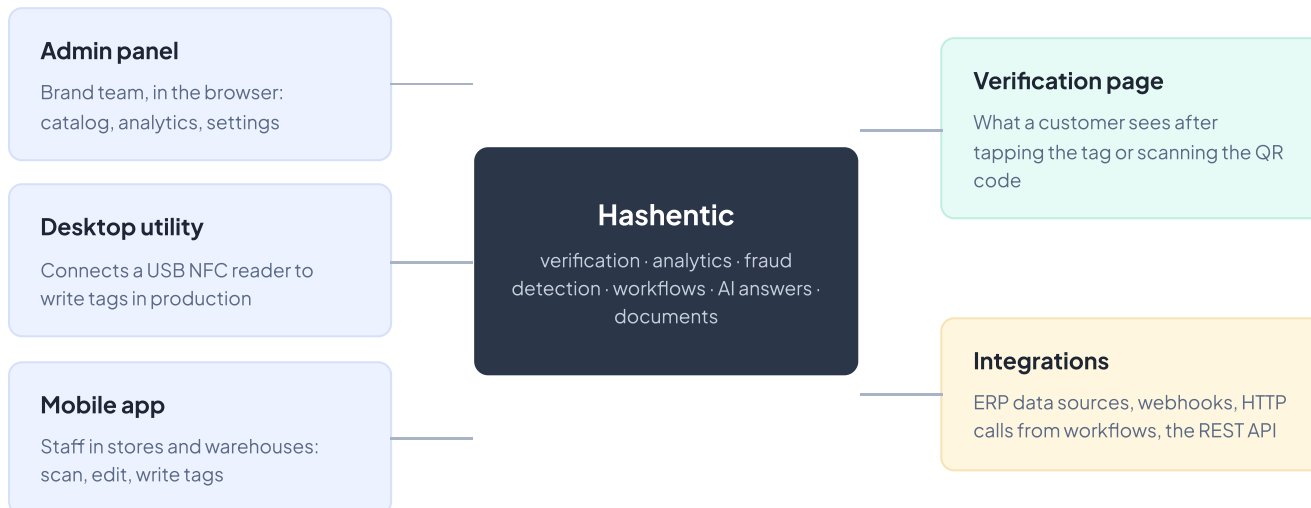
02 Key concepts

03 Roles, permissions and your license

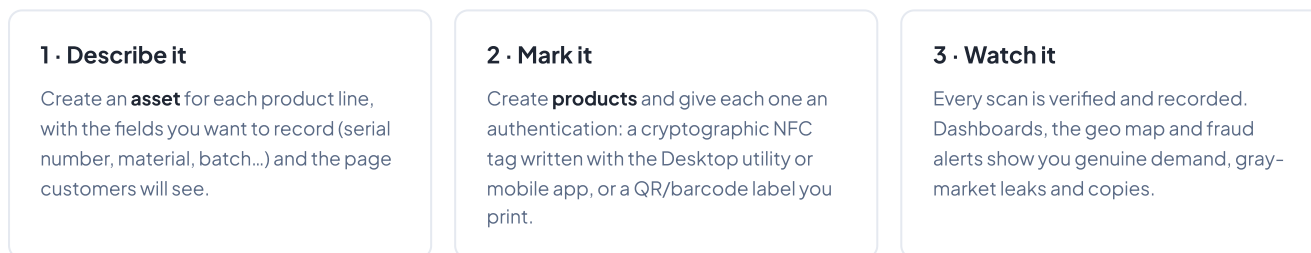
04 Finding your way around

1 Hashentic at a glance

Hashentic gives every physical product a digital identity that customers can check in one tap. You define your product lines, mark each item with a secure NFC tag or a QR code, and Hashentic verifies every scan, shows the customer a branded page, and tells you where, when and how your products are being checked.



How a product gets protected



What you can do with it

- ✓ Authenticate products with **NTAG 424 DNA** and **EM4425** secure NFC tags, **NTAG 215** tags, or QR/DataMatrix/Code 128 barcodes, including GS1 Digital Link.
- ✓ Track every **valid and invalid scan** with date, country, device and risk flags.
- ✓ Write tags one by one or **in bulk** from a spreadsheet or an ERP, and print barcode sheets as PDF.
- ✓ Collect warranty registrations and sign-ups with **forms** on the verification page.
- ✓ Control access with **roles and fine-grained permissions**, two-factor sign-in and a full audit log.
- ✓ Design branded **verification pages** from a gallery of 60+ templates, with an AI assistant and product documents on the page.
- ✓ Detect **cloned tags, impossible travel, gray-market sales** and scan bursts automatically.
- ✓ Automate reactions with **workflows**: block a tag, label a product, notify the team, call your systems.
- ✓ Prepare **Digital Product Passport** data (GS1, economic operator, circularity, EU battery passport).
- ✓ Use the admin panel in **six languages**: English, German, Spanish, Polish, Russian and Chinese.

i About the examples in this guide

All screenshots come from a demo workspace for a fictional brand, **Kestrel & Vine**, which sells watches, leather goods and a fragrance. Names, numbers and scans are invented. Your screens show your own catalog, and some menus appear only if your license and permissions include them.

2 Key concepts

A few terms come up on almost every screen. Learn these and the rest of the admin panel reads naturally.

Asset

A product line or model, such as "Heritage Chronograph 42". It defines the fields every item carries, the verification page design, fraud rules, forms and workflows. An asset can be limited to a fixed number of products.

Product

One physical item of an asset, with its own values (serial number, batch...) and a short **identifier** such as **7eWb86L**. Products can be blocked or deleted.

Authentication

The carrier that proves a product is genuine: an NFC tag (NTAG 424, NTAG 215, EM4425) or a barcode/QR code. A product can have more than one.

Verification

One scan of an authentication by anyone. It is either **valid** or **invalid**, with a reason such as "Invalid CMAC" or "Product is blocked".

Field

A piece of product data defined on the asset: Text, Email, Number, Select, Lookup, Date or Checkbox. Fields can be required, protected (encrypted), hidden from consumers, or editable later.

Preset

A reusable bundle of fields and a page template. Pick a preset when creating an asset to start from the same structure every time.

Lookup

A managed list of values (materials, boutiques, markets...) that Lookup fields draw from, so everyone uses the same spelling.

Label

A colored tag on a product or authentication, such as "Sold" or "In service". Labels drive templates, forms and workflows.

Template

The verification page a customer sees. Each asset has a verified page, an optional unverified page and optional **auth templates** for specific countries, labels or tag types.

Workflow & form

Workflows react to events (a scan, a block, a fraud alert, a form, a webhook) with actions. Forms collect customer input on the verification page.



Tags vs. barcodes in one sentence

Secure NFC tags (NTAG 424 DNA, EM4425) generate a new cryptographic code on every tap, so a copied link is detected.

Barcodes and NTAG 215 tags carry a fixed link: they are cheaper and printable, but a photocopy scans as genuine. Use fraud alerts (velocity, gray market) to watch them.

3 Roles, permissions and your license

What a person can see and do depends on two things: the **permissions** on their account and the **features** in your company's license. If a menu item described in this guide is missing, one of the two is the reason.

Roles

Role	What it means
Super User	The highest role, held by the built-in administrator account. Has every permission, sees every asset and is the only role that can open the Audit log. A Super User can give this role to other accounts.
Admin	Sees all assets. Can do exactly what the permissions ticked on the account allow.
User	Works only with the assets assigned to the account, within its permissions.
Authority · Recycler · Repairer	Partner roles for the Digital Product Passport. They read, update and block products of assigned DPP assets, and see or edit only the fields whose data audience includes their role.

Permissions

On the user form permissions are grouped by area: Products, Assets, Presets, Lookups, Workflows, AI, Users, Settings, License, Integrations and Notifications management (see [Users and access](#)). Granting a write permission also grants the matching read permission. The most important ones:

Group	Permissions
Products	Read · Write · Update · Delete · Block · Unblock products; read valid and invalid verifications; read/write bulk operations; read/write fraud alerts
Assets, presets, lookups	Read · Write assets, Delete assets; Read · Write presets; Read · Write lookups
Workflows	Read · Write workflows; Write workflow templates; Read audit events
AI	Generate AI fields, template, recommendations and workflows; Use AI analysis; Use AI assistant; Read customer questions
Administration	Read · Write users; Read · Write settings; Write license; Manage ERP connections; Read notifications

License features

Your license sets limits (users, assets, tags, barcodes, AI tokens, document storage...) and switches on optional features. Throughout this guide, features that need a license option are marked with a **License feature** chip.

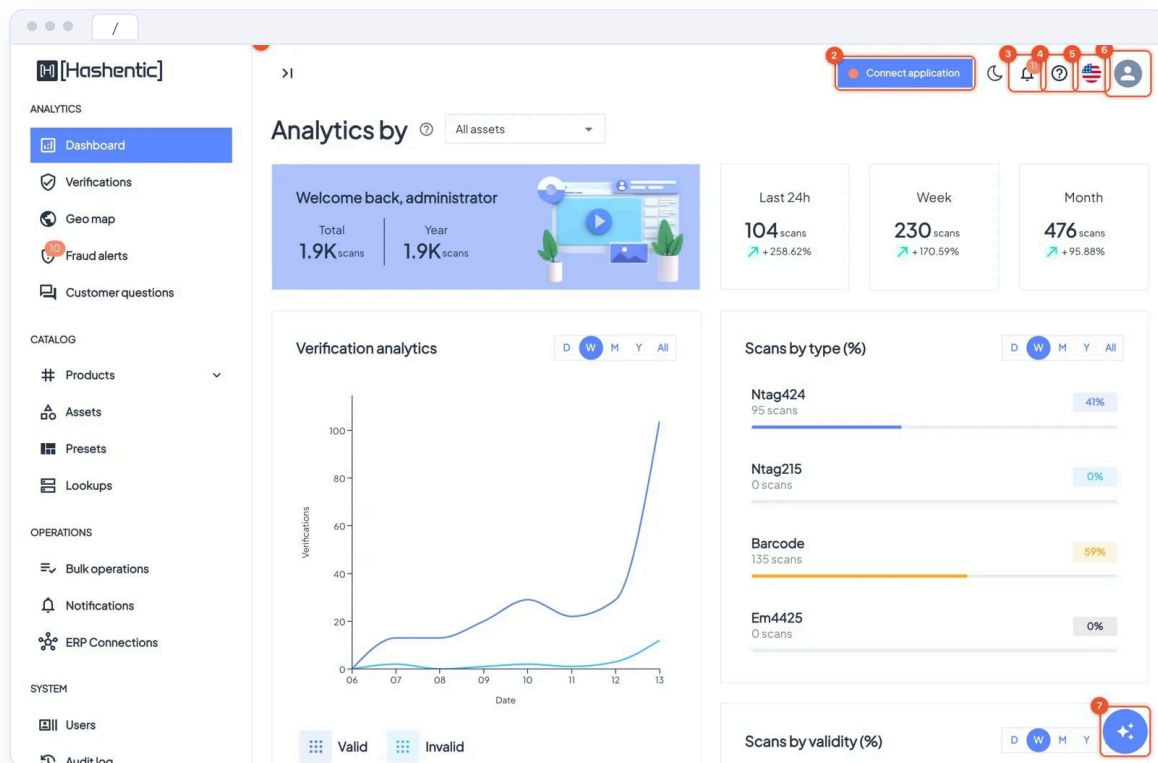
Feature	What it unlocks
Bulk write	Multiple mode for writing tags and generating barcodes, Bulk operations, ERP connections
Update records	Editing product values after creation
Geolocation analytics	Country of each scan, Geo map, country rules in templates and fraud detection

Feature	What it unlocks
Device info analytics	Device, brand, model and OS of each scan
Fraud detection	Fraud alerts, fraud settings, the "On fraud detected" workflow trigger
Workflows · Asset forms	Workflow builder and runs · forms on the verification page
AI · AI analysis · AI assistant · Customer AI	AI generators · questions over your data · the assistant in the admin panel · AI answers on the verification page and the Customer questions page
Product documents	Document library and documents on the verification page
Product lookup	Filling GS1 data from a GTIN when creating an asset
White-label branding	The Branding page: your own name, logos, colors and links
Mobile applications	The mobile app, sign-in by QR code, tag writing from a phone

Your license may also restrict which carrier types (NTAG 424, NTAG 215, EM4425, Barcode) you can use. The [License page](#) shows your license status, dates, limits and current usage; ask your administrator which features are included.

4 Finding your way around

The admin panel works in any modern browser. The menu on the left is grouped by task; the bar at the top holds the tools you need on every page.



The admin panel. 1 Menu, grouped into Analytics, Catalog, Operations and System · 2 Reader status: connects the Desktop utility for NFC tags · 3 Notifications · 4 Replay the guided tour · 5 Language · 6 Your profile · 7 AI assistant.

The menu

- **Analytics:** Dashboard, Verifications, Geo map, Fraud alerts, Customer questions.
- **Catalog:** Products (List, Add new, Update), Assets, Presets, Lookups.
- **Operations:** Bulk operations, Notifications, ERP Connections.
- **System:** Users, Audit log, Applications, Settings, Branding, License.
- At the bottom: **Integration guide**, **Mobile app**, **Setup desktop utility** and theme settings.

Handy everywhere

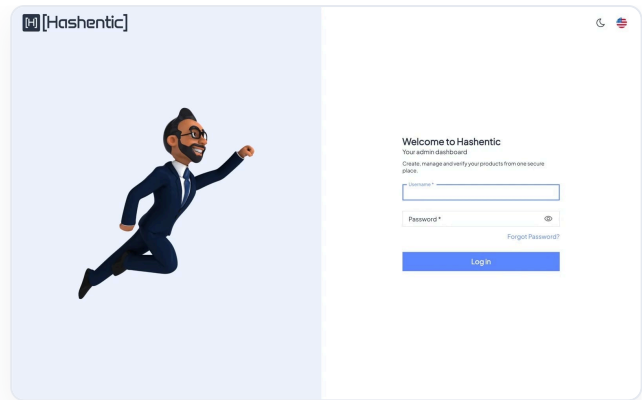
- The **?** next to a page title explains the page; **Show app tour** replays the guided tour.
- Lists share the same tools: a search box, **Add filter** for precise filters, sortable columns and page size.
- Switch **light/dark** mode with the moon icon and the **language** with the flag.
- The **sparkle button** at the bottom right opens the AI assistant.

Signing in

Open your company's Hashentic address and sign in with your username and password. Depending on your company's settings you may also see **Continue with Google**, and you may be asked for a code from your authenticator app (two-factor authentication).

Forgot your password? Click **Forgot Password?** and follow the link sent to your email. After several failed attempts the account is locked for a few minutes.

The first time you sign in, a short tour points out the main areas. You can replay it any time.



Sign-in page. Your company's brand name appears in the title.



Feature catalog

Every area of Hashentic, one chapter each: what it is for, what you see on screen and what you can do there. Use it as a reference; the step-by-step guides in Part III build on it.

05 Dashboard

06 Verifications

07 Geo map

08 Fraud & anomaly alerts

09 Customer questions

10 Products

11 Assets and fields

12 Verification page templates

13 Presets and lookups

14 Labels and forms

15 Workflows

16 Writing tags and printing barcodes

17 Bulk operations and ERP

18 Notifications and audit log

19 AI features

20 Users and access

21 Settings, branding and license

22 Mobile app and Desktop utility

23 The consumer verification page

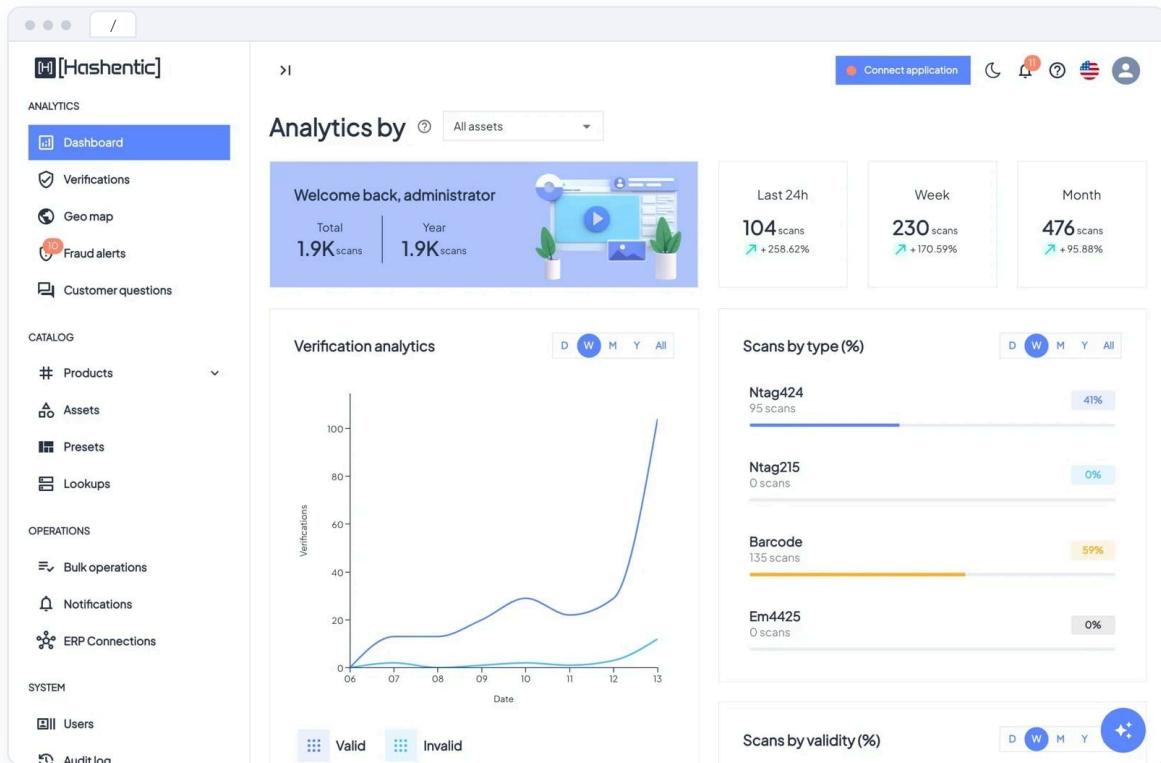
5 Dashboard

The home page: how many genuine scans you get, how that is trending, which carriers customers use and where they are.

Menu Analytics → Dashboard

Access everyone; data limited to your assets

License Geolocation analytics for the country map



Dashboard. Pick an asset in **Analytics by** to narrow every card to one product line.

- ✓ **Welcome card** with **Total** and **Year**, plus **Last 24h**, **Week** and **Month** cards with the trend against the previous period. These count genuine (valid) scans.
- ✓ **Scans by type (%)**: the share of NTAG 424, NTAG 215, EM4425 and barcode scans.
- ✓ **Scans by country**: a world map shaded by genuine scans per country.
- ✓ **Verification analytics**: valid and invalid scans over time. Switch the period with **D W M Y All**.
- ✓ **Scans by validity (%)**: genuine vs. failed checks.
- ✓ **Drill down anywhere**: click a number, a chart series, a type row, a pie slice or a country to open the list of the scans behind it.

Tip

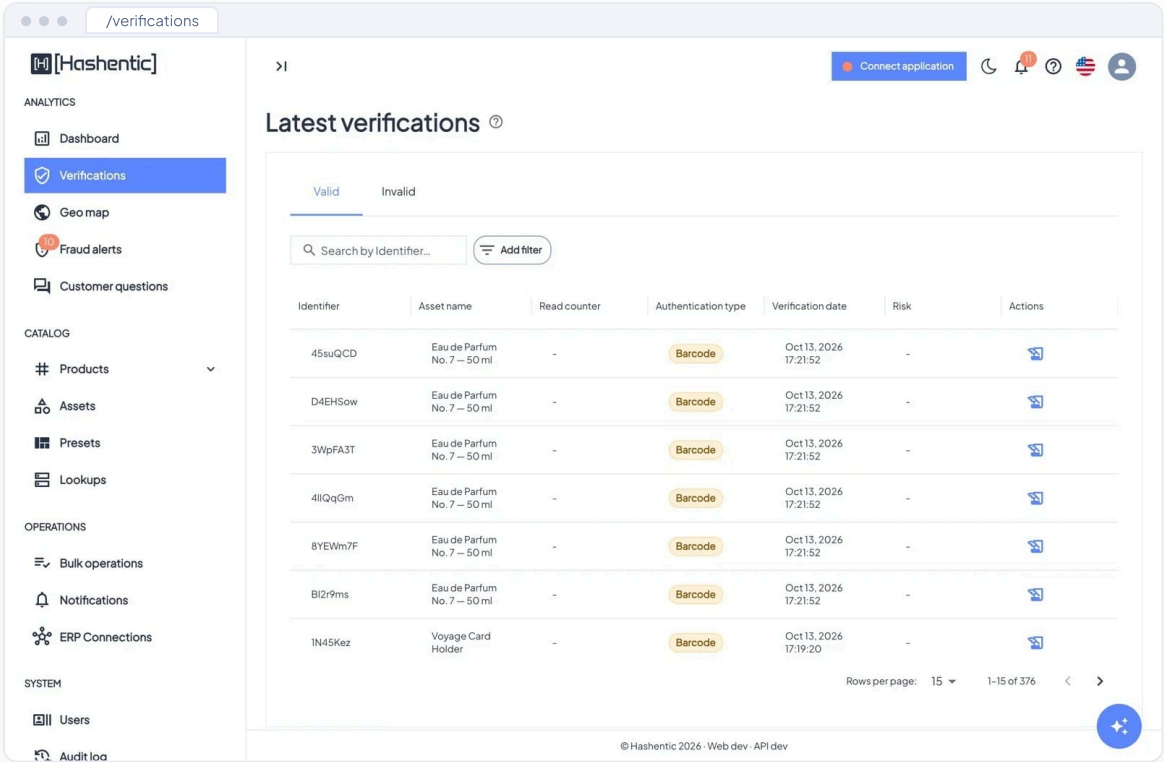
The drill-down list shows every individual scan, with the context you clicked on as fixed filter chips (for example "Country: FR"). Click a row to open its full verification details.

6 Verifications

The log of scans. Valid shows genuine checks, Invalid shows every scan that failed and why.

Menu Analytics → Verifications

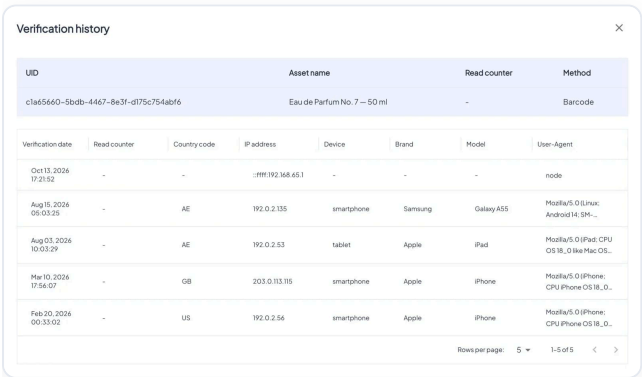
Permission Read valid / invalid product verifications



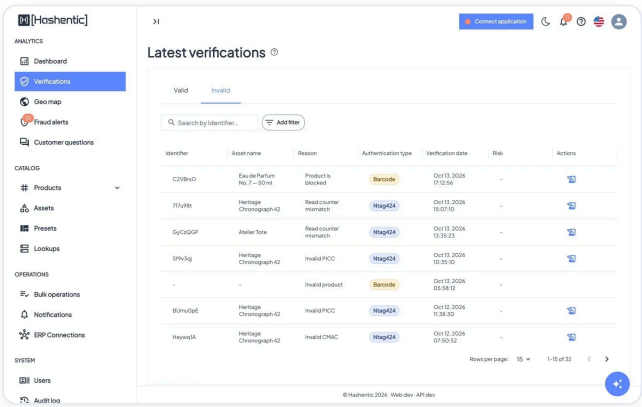
Latest verifications. The list shows the most recent matching scan of each product. Use the clock icon for every scan of a tag, or the Dashboard drill-down for every scan in a period.

Why do scans fail?

Most failures are copies: a cloned NFC tag fails its cryptographic check ("Invalid CMAC", "Invalid PICC"), a re-shared tag link is caught as "Already verified" or "Read counter mismatch", and a made-up or deleted code is an "Invalid product". Scans of blocked products fail with "Product is blocked" or "This authentication has been blocked".



Verification history of one QR code: date, country, IP address and device of every scan.



Invalid tab. The Reason column explains each failure. All reasons are listed in Appendix A.

Columns

- **Identifier** and **Asset name** of the product.
- **Read counter** of NFC tags, which rises with every tap ("–" for barcodes). On the Invalid tab this is the **Reason**.
- **Authentication type**: Ntag424, Ntag215, Em4425 or Barcode.
- **Risk**: **VPN**, **Proxy**, **Tor** or **Threat** when the scan came from a flagged network.

Finding scans

- Search by identifier, or use **Add filter**: Identifier, UID, Authentication type, Verification date, Asset name, Country code, and on the Invalid tab, Reason.
- Click a row for **Verification info**: country, IP address, device, brand, model, browser and the product's field values.
- The clock icon opens the **Verification history** of that tag or code: every scan, in order.

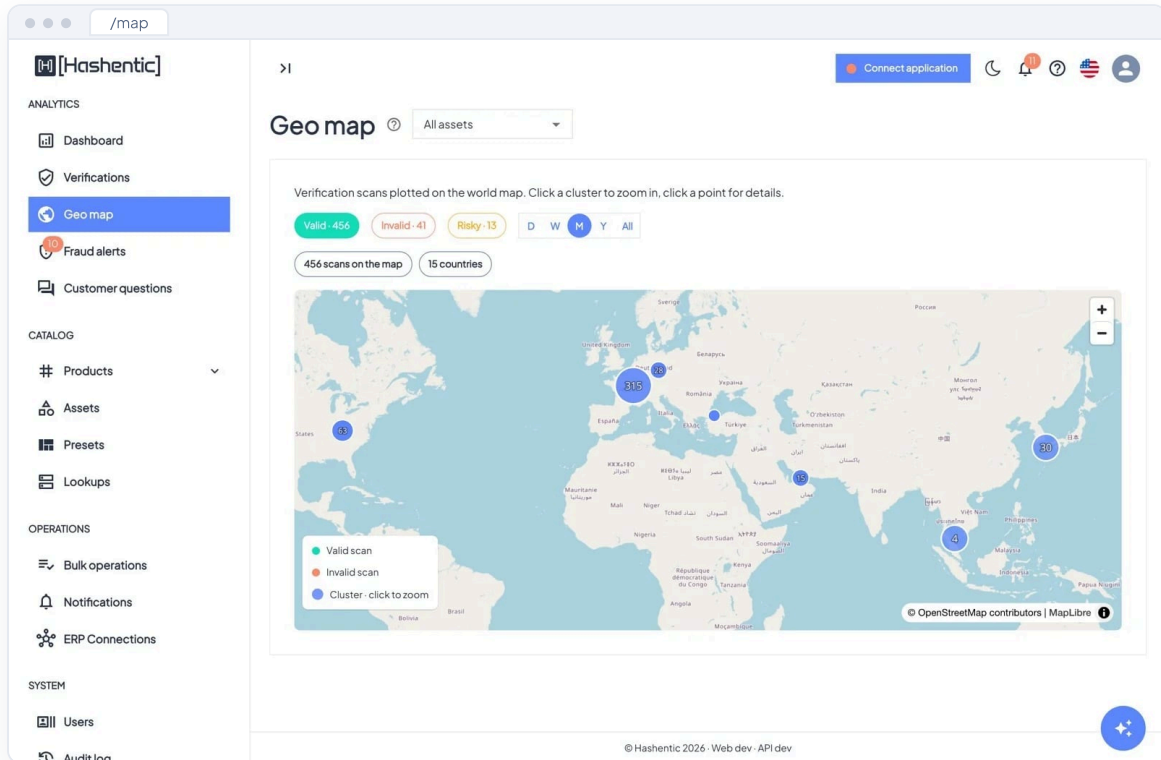
7 Geo map

Every geolocated scan on an interactive world map, so you can see where your products are checked, and where copies surface.

Menu Analytics → Geo map

Permission Read verifications

License Geolocation analytics



Geo map. Nearby scans merge into clusters; click a cluster to zoom in and a point to see the list of scans.

- ✓ Toggle **Valid**, **Invalid** and **Risky** scans. Invalid and risky (VPN, proxy, Tor, threat) scans are hidden until you switch them on.
- ✓ The chips above the map count the scans shown and the countries they come from.
- ✓ Choose the period (default **M**, the last month) and narrow to one asset.
- ✓ Click a point, then **Click to see the list** to open the scans behind it.

8 Fraud & anomaly alerts

Hashentic watches the stream of scans and raises an alert when a pattern looks like counterfeiting or diversion. The menu badge shows how many alerts are still **New**.

Menu Analytics → Fraud alerts

Permission Read fraud alerts (actions: Write fraud alerts)

License Fraud detection

Detected	Severity	Signals	Score	Asset	Country	Status	Actions
Oct13, 2026 17:22:30	Medium	Invalid-scan burst	25	Eau de Parfum No. 7 – 50 ml	AE	Confirmed	✕
Oct13, 2026 17:22:29	Medium	Impossible travel	40	Heritage Chronograph 42	US	New	✓ ⚠
Oct13, 2026 17:22:29	High	Cloned chip (counter)	50	Atelier Tote	IT	New	✓ ⚠
Oct13, 2026 17:22:29	Medium	Gray market	35	Heritage Chronograph 42	CN	Acknowledged	⚠ ✕
Oct13, 2026 17:22:29	Critical	Cloned chip (counter) Impossible travel	90	Heritage Chronograph 42	TR	New	✓ ⚠
Oct13, 2026 17:22:29	Medium	Impossible travel	40	Eau de Parfum No. 7 – 50 ml	FR	New	✓ ⚠
Oct13, 2026 17:22:29	Medium	Velocity spike	30	Voyage Card Holder	ES	Dismissed	⚠

Fraud & anomaly alerts. Each alert combines one or more signals into a score and a severity.

What triggers an alert

Signal	Raised when...	Weight
Cloned chip (counter)	A secure NFC tag reports a read counter that is not higher than one already seen: two physical tags share the same identity.	50
Impossible travel	Two consecutive scans of the same tag are more than 100 km apart and would need more than 900 km/h to travel.	40
Gray market	At least 3 genuine scans of an asset within 24 hours come from a country outside the asset's Authorized regions .	35
Velocity spike	The same tag or code is scanned at least 10 times within 10 minutes.	30
Invalid-scan burst	A product collects at least 5 failed scans within 30 minutes.	25
Risky IP	Added to another signal when a triggering scan came from a VPN, proxy, Tor or threat network.	15

The score is the sum of the weights (at most 100). From 75 an alert is **Critical**, from 45 **High**, from 25 **Medium**. The High and Critical cutoffs and the travel, velocity, gray-market and burst-window values can be tuned in [Settings → Fraud & anomaly detection](#); the burst count uses *Invalid verification anomaly threshold* under Verification alerts. High and Critical alerts also send a notification and can start a workflow ("On fraud detected").

Fraud alert

Critical

Score: 90

New

Signals

Cloned chip (counter)

Impossible travel

Asset

Heritage Chronograph 42

Country

TR

Window

Jan 18, 2026 19:07:20 — Oct 13, 2026 16:58:56

Metrics

Speed (km/h): 1253.4

Distance (km): 2256.5

Read counter: 11

Counter drop: 7

Previous read counter: 18

Triggering scans

Verification date	Country	Coordinates	Read counter
Oct 13, 2026 16:58:56	TR	41.018, 28.975	11

Confirm fraud

Dismiss

Acknowledge

Close

Alert details. Metrics (distance, speed, counters) and the scans that triggered it.

Working an alert

- **Acknowledge** : you have seen it and are looking into it.
- **Confirm fraud** : it is a real case.
- **Dismiss** : a false alarm.

A status only records who decided and when. Confirming does not block anything by itself: block the product or tag on its page, or let a workflow do it.

Filter with **Add filter** by Severity, Status, Signals, Detected date, Asset and Country.

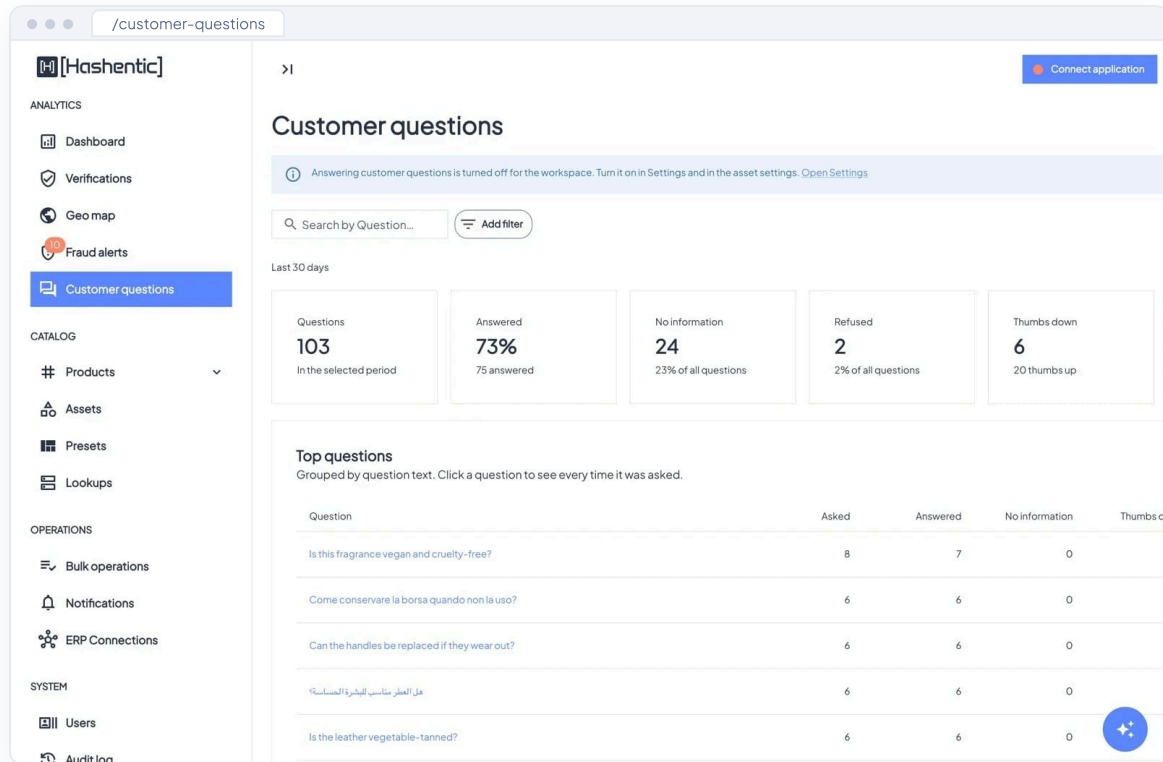
9 Customer questions

Customers who verify a genuine product can ask an AI assistant about it on the verification page: care, warranty, ingredients. This page shows what they ask and how well it was answered, so you can close the gaps in your product information.

Menu Analytics → Customer questions

Permission Read customer questions

License AI + Customer AI



Customer questions. Summary tiles filter the list; **Top questions** groups repeated questions.

- ✓ Tiles for **Questions**, **Answered**, **No information**, **Refused**, **Thumbs down** and **From cache**. Click one to filter.
- ✓ **All questions** lists time, asset, product, language, status, cited sources, the customer's feedback and country.
- ✓ **Top questions** groups identical questions with how often they were asked and answered.
- ✓ Filter by asset, period (7/30/90 days or custom), language, status and feedback.

Status	Meaning
Answered	The assistant answered from the product's public fields, passport data and public documents.
No information	Your data does not contain the answer. Add a document or fill in a field to close the gap.
Refused	Out of scope: authenticity claims, unrelated topics, personal data or attempts to change the assistant's rules.
Failed	The AI service was temporarily unavailable.

i Turning it on

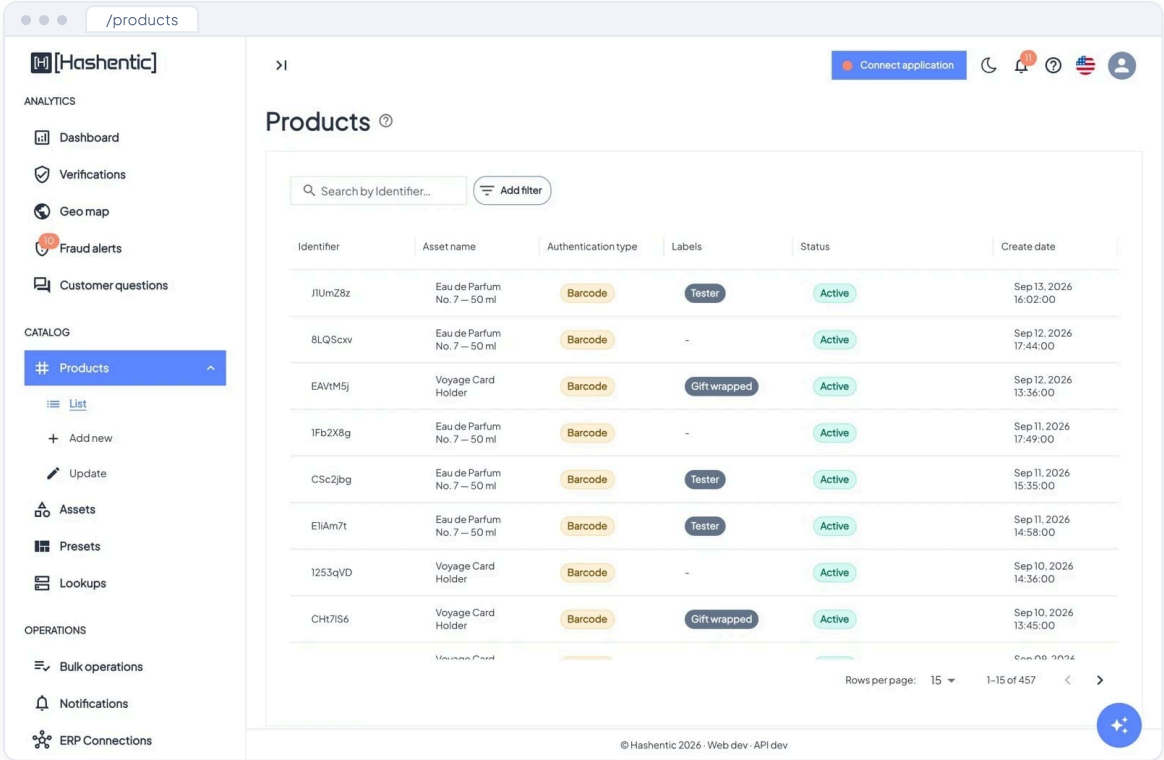
Two switches are needed: **Settings** → **Answer customer questions on the verification page** for the whole workspace, and **Answer customer questions with AI** on each asset's Settings tab, where you can also write a welcome text. The page is read-only and lists questions, not answer texts. Answers are cached for reuse (answered questions for 7 days), which is what the *From cache* tile counts.

10 Products

Every tagged item you have issued. Find any product in seconds, see its scans and history, edit its data, print its code, or block it.

Menu Catalog → Products → List

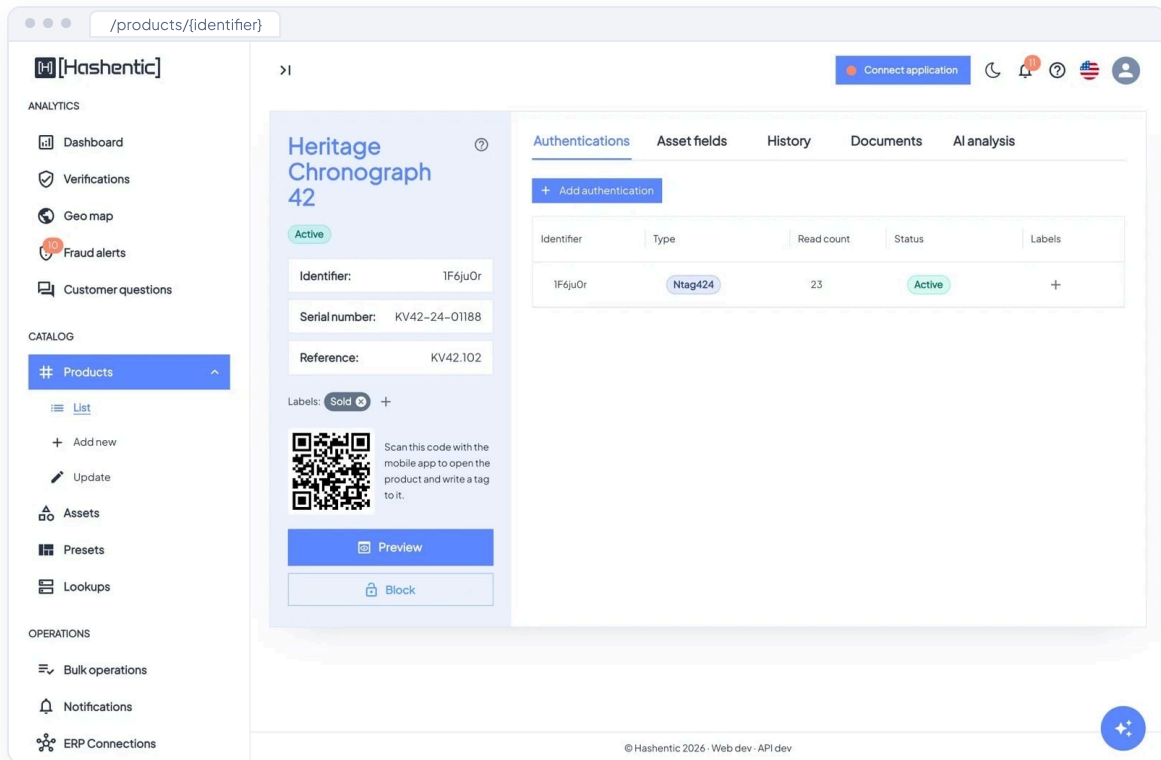
Permission Read products



Products. Columns: Identifier, Asset name, Authentication type, Labels, Status and Create date. Fields marked *Show in grid* appear as extra columns on the asset's Products tab.

Search by identifier or use **Add filter** for Identifier, UID, Authentication type, Labels, Deleted, Blocked and Create date. Under **Products** in the menu you also find **Add new** (create and tag products, see [chapter 16](#)) and **Update** (scan products to edit them, alone or in bulk).

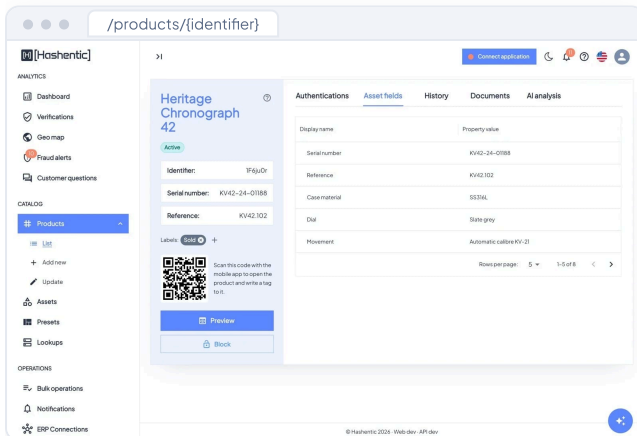
The product page



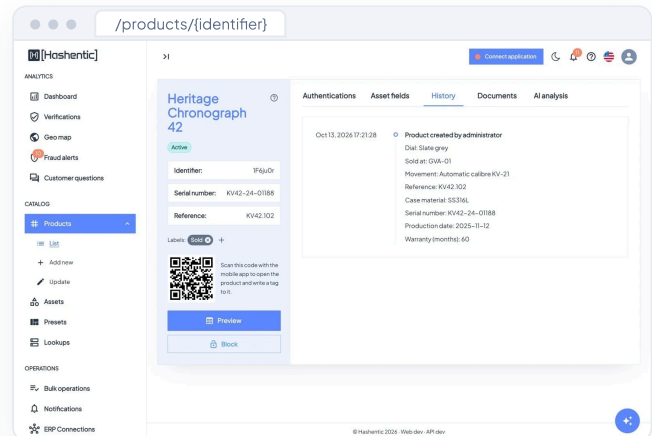
Product page. On the left: status, key values, labels and a QR code for the mobile app. On the right: tabs.

! Blocking vs. deleting

Block a product when it is stolen, recalled or suspected to be copied: customers who scan it see the "not verified" page, and you can unblock it later. You can also block a single tag on the Authentications tab and keep the product's other tags working. Locked NTAG 215 products cannot be deleted from the admin panel.



Asset fields tab: the product's values.



History tab: every change with author and time.

Tabs

- **Authentications:** the tags and codes of the product with their type, read count, status and labels. Add another one with **Add authentication**; block, unblock, remove one, download its barcode or give it its own page template.
- **Asset fields:** the product's values.
- **History:** who created and changed the product, and what changed.

Actions

- **Preview** shows the verification page exactly as a customer would see it.
- **Edit** changes values of fields that allow updates.
- For products with secure NFC tags, Edit, Block and Delete appear after tapping the tag (**Products** → **Update**) or when the asset allows unprotected management. Single tags can always be blocked on the Authentications tab.

- **Documents:** files for this one item (certificate, service record).
- **AI analysis:** ask questions about this product's scans ([chapter 19](#)).

- **Download** exports the barcode as PDF, CSV, XLSX or TXT.
- **Block** / **Unblock**: a blocked product fails every verification.
- **Delete** removes the product from use; it stays in the records as deleted.
- **QR for the mobile app** opens the product in the mobile app, for example to write a tag to it.

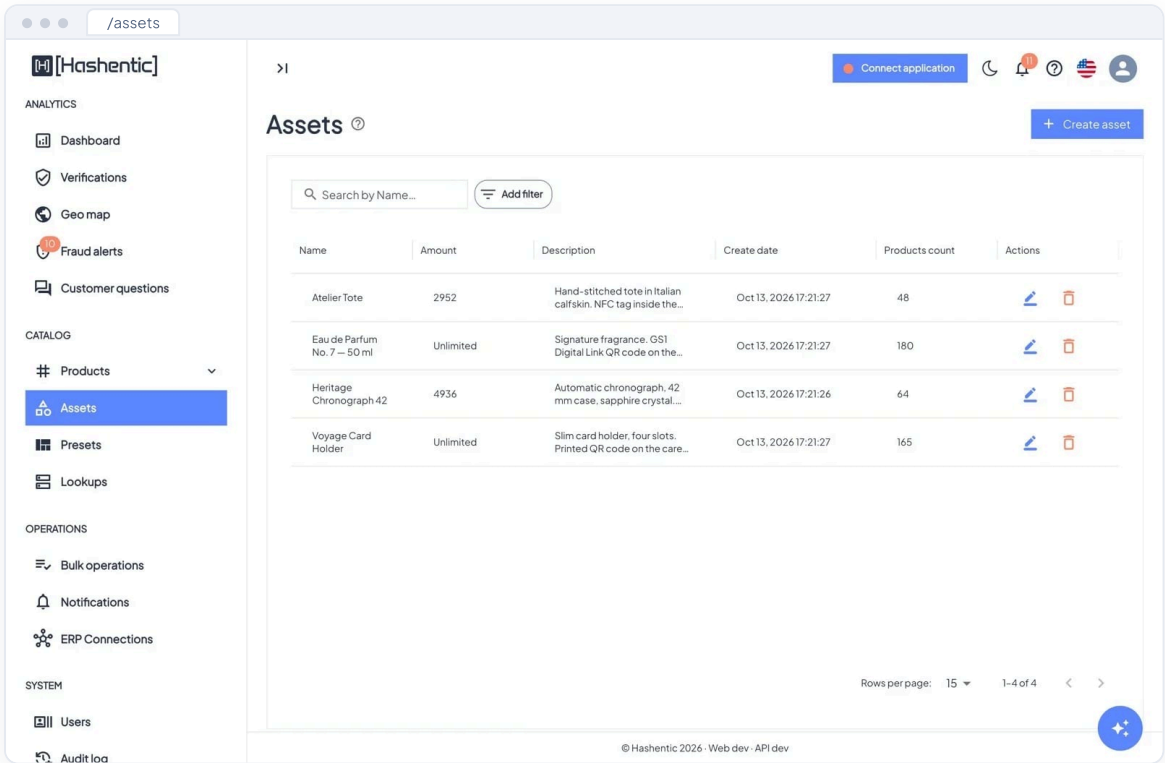
11 Assets and fields

An asset is a product line: the blueprint every item of that line follows. Its page brings together the fields, the verification page, documents, labels, forms, workflows and fraud rules of the line.

Menu Catalog → Assets

Permission Read / Write / Delete assets

Limit number of assets in your license



Assets. Amount shows how many products may still be created ("Unlimited" for open-ended lines) and Products count how many exist.

Creating an asset

Create asset

Manual

AI Powered

1 General

Name *

Emission ⓘ

☐ Limited ⓘ

Use preset ⓘ

Description

☐ DPP compliant ⓘ

☐ GS1 compliant ⓘ

☐ Battery passport (EU Battery Regulation) ⓘ

Back

Create

Cancel

Create asset opens a short form: **Name** (at least 4 characters), an optional **Amount** with **Limited** to cap the number of products, an optional **preset** to copy fields and a template from, and a **Description**.

Three options add compliance steps to the form:

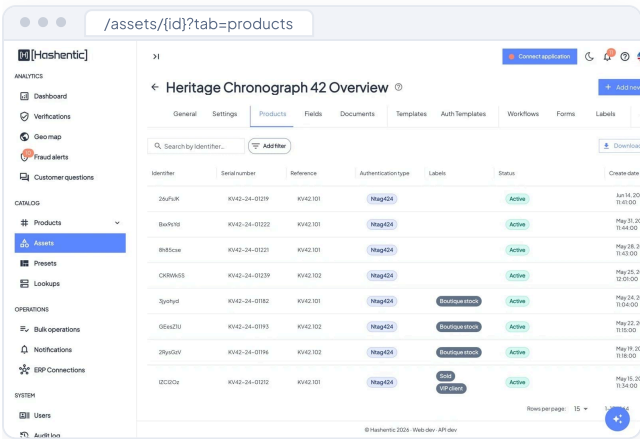
- GS1 compliant:** GTIN, brand name, trade item description, net content and target market, with **Find product by GTIN** to fill them in.
- DPP compliant:** Digital Product Passport data, the economic operator and circularity & sustainability information.
- Battery passport (EU Battery Regulation):** adds the battery passport fields.

The **AI Powered** tab drafts the fields and a page template from a short description of the product.

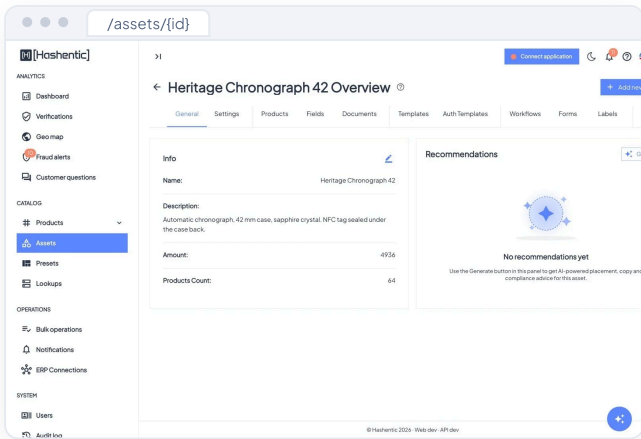
Create asset: Manual or AI Powered.

The asset page

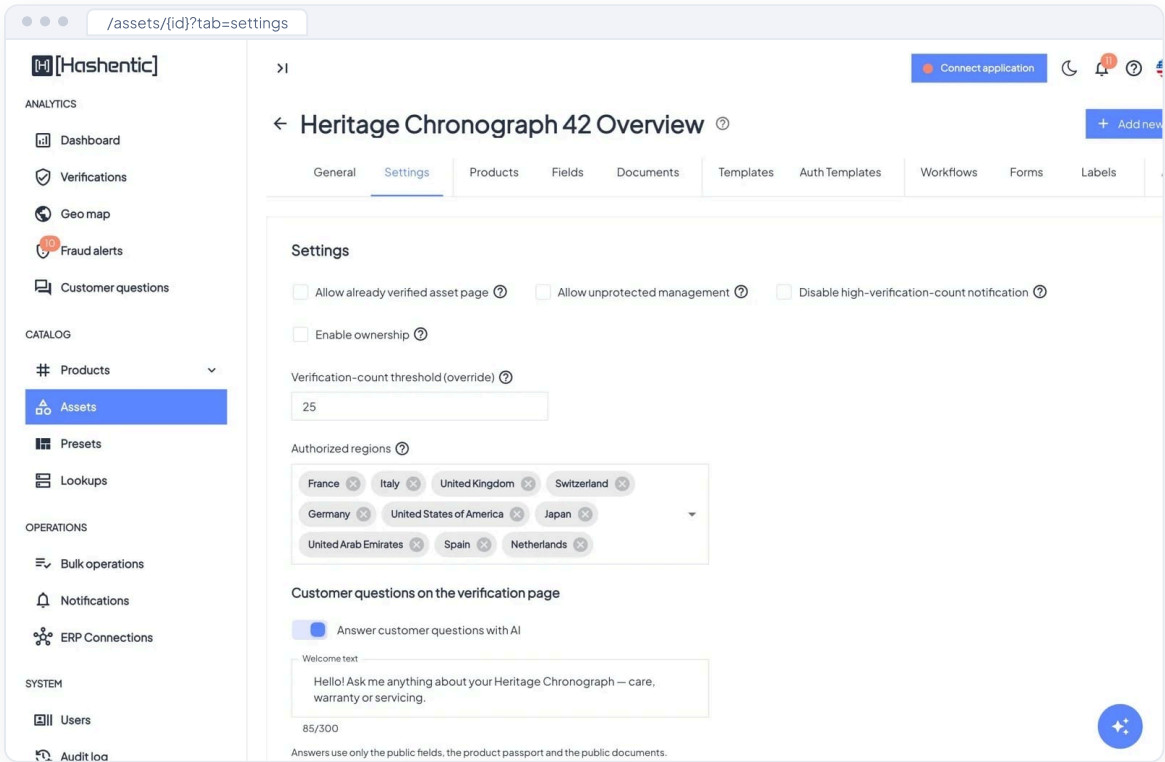
Tabs:
 [General](#)
[Settings](#)
[Products](#)
[Fields](#)
[Documents](#)
[Templates](#)
[Auth templates](#)
[Workflows](#)
[Forms](#)
[Labels](#)
[AI analysis](#)
 . The button [Add new product](#) at the top starts tagging with this asset already selected.



Products tab: this line's items, filters and [Download barcodes](#) for the filtered set.



General tab: name, description, amount, and [AI Recommendations](#) for protecting the line.

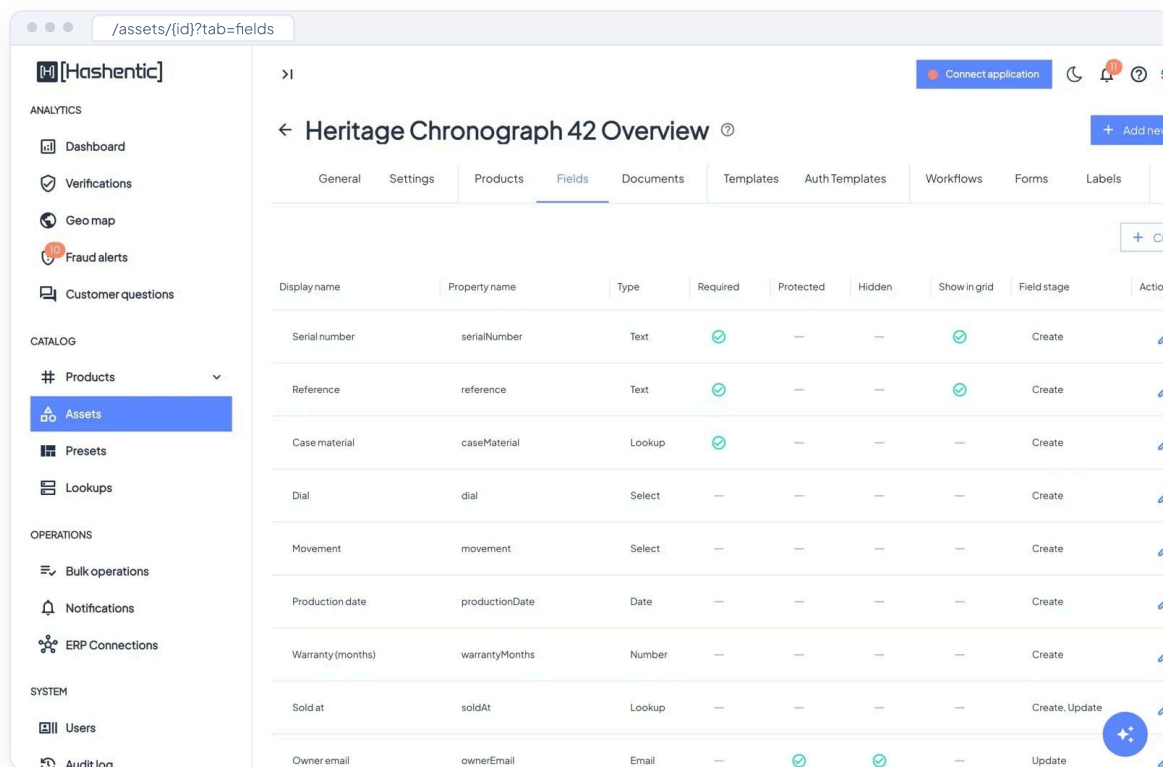


Settings tab. Authorized regions feed gray-market detection; the customer questions section switches on the AI assistant for this line.

Asset setting	What it does
Allow already verified asset page	When a secure tag link is opened again, a designed page is shown with the notice "Product is not verified. Current url used more than once." instead of the failure page. Useful when customers re-open the page to look up product info.
Allow unprotected management	Lets staff update, block or delete products with secure NFC tags without tapping the tag, and makes the asset available for bulk updates by query.
Disable high-verification-count notification / threshold	Controls the notification sent when one tag is scanned unusually often.
Authorized regions	Countries where this line is sold. Repeated genuine scans elsewhere raise a <i>Gray market</i> alert.

Asset setting	What it does
Answer customer questions with AI · Welcome text	The AI assistant on this line's verification page and its greeting.
Enable ownership	Records product ownership (with the Product ownership license feature).

Fields



Fields tab. The data every product of the line carries.

Asset field — Case material

Attributes

Display name *

Case material

Property name

caseMaterial

Type

Lookup

Lookup

Case materials

Options

☒ Required
 ☐ Protected
 ☐ Hidden
 ☐ Show in grid

Field stage

☒ Create
 ☐ Update

Data audience (DPP)

☒ Public
 ☐ Authority
 ☐ Recycler
 ☐ Repairer

Submit

Cancel

Field settings for a Lookup field.

Types: Text, Email, Number, Select (your own list of options), Lookup (values from a [lookup](#)), Date and Checkbox, each with its own checks (length, pattern, min/max, only past or future dates).

Options

- Required** : must be filled.
- Protected** : stored encrypted and excluded from search. Use it for personal data such as an owner's email.
- Hidden** : not shown to customers on the default page.
- Show in grid** : a column in the asset's product list.

Field stage: **Create** fields are filled when the product is made; **Update** fields can be changed later (for example "Sold at").

Data audience decides which Digital Product Passport partners (Authority, Recycler, Repairer) may see a field.



Once products exist

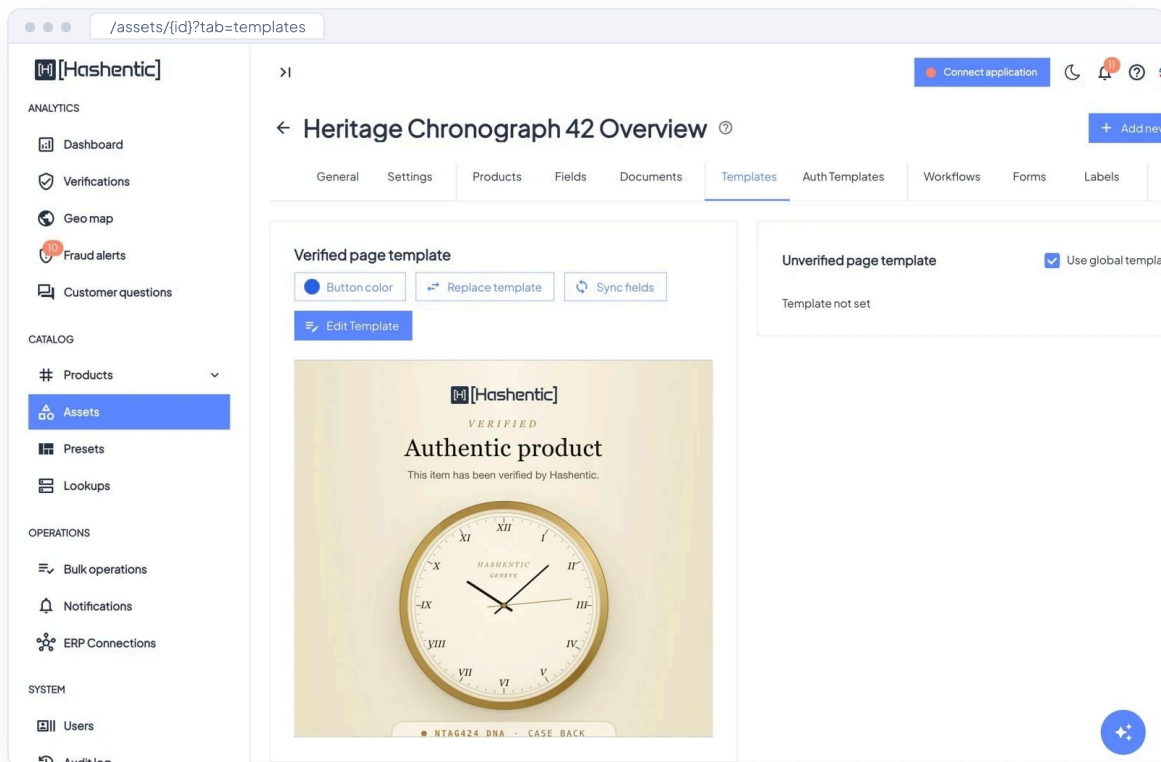
The property name of a field is fixed when it is created. As soon as an asset has products, fields can no longer be deleted (you can still add and edit them). Plan the structure on a test asset first, or save it as a preset.

12 Verification page templates

The page your customer lands on after a scan is your brand moment. Each asset decides what it looks like when the product is verified, and when it is not.

Where Asset → Templates tab; Settings → Unverified page template

Permission Write assets



Templates tab. The verified page on the left, the unverified page on the right.

Ways to build a page

Templates gallery

60+ ready designs, from minimal and editorial styles to industry pages for watches, bags, cosmetics, wine, pharma or batteries, and Digital Product Passport layouts. Filter by style, use case and layout, preview in light or dark, pick the fields to show, and apply.

Block builder

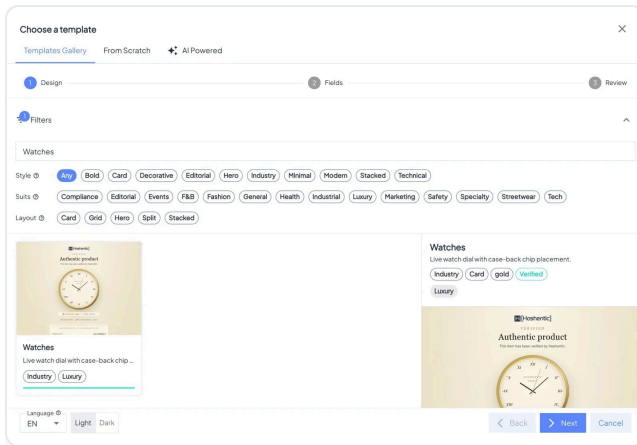
A drag-and-drop editor (**Edit Template**) with headings, text, images, buttons, columns and dividers, and desktop/mobile preview.

Custom HTML

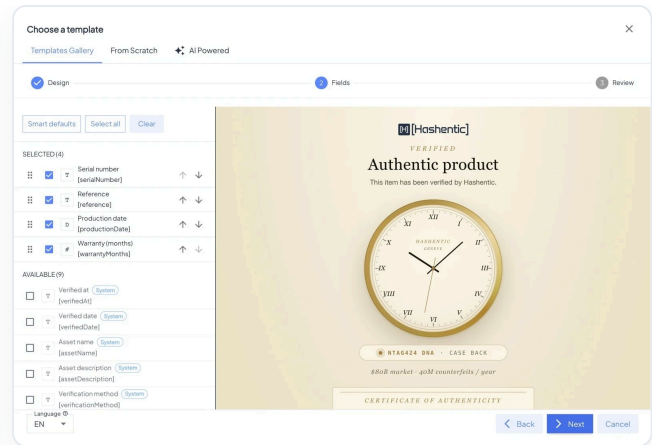
Your own HTML and CSS, with placeholders such as **[AssetName]**, **[VerifiedAt]** or any field like **[serialNumber]** (see Appendix B).

External website · AI Powered

Show a page from your own website, or let AI generate a template for the asset. You can also copy the template of another asset.



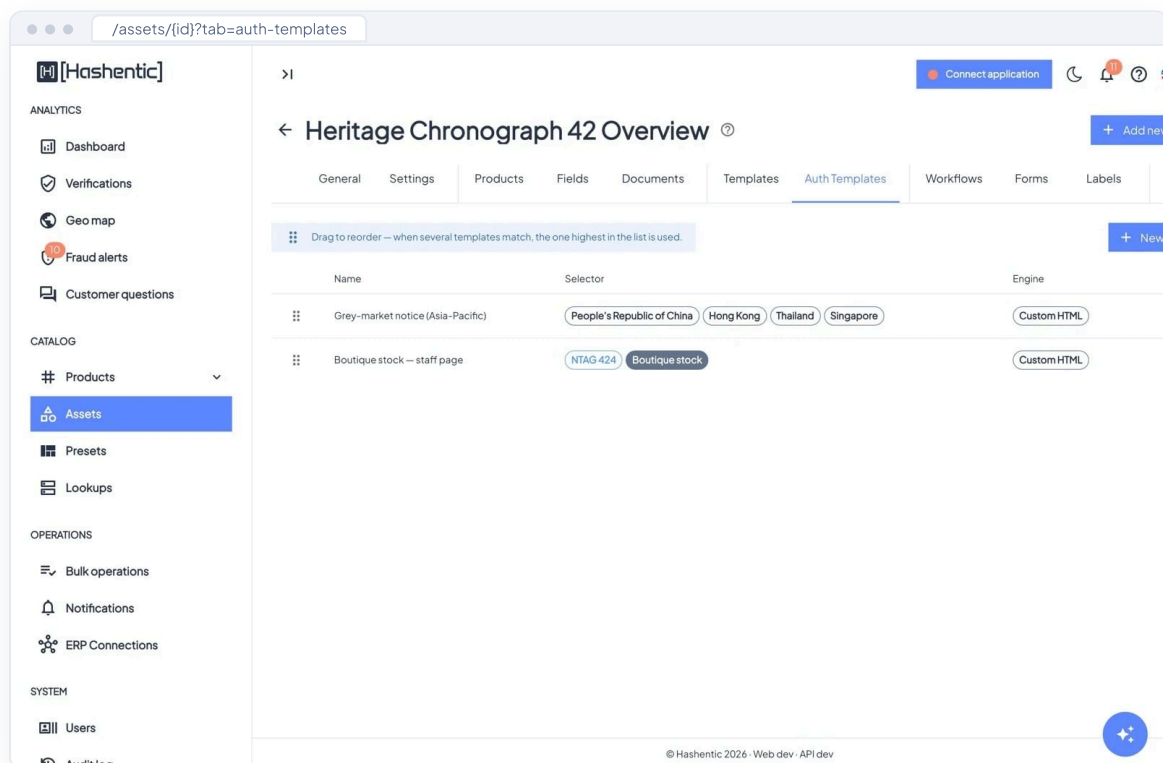
Choose a template: pick a design and preview it.



Fields step: choose and order the fields shown on the page.

More control

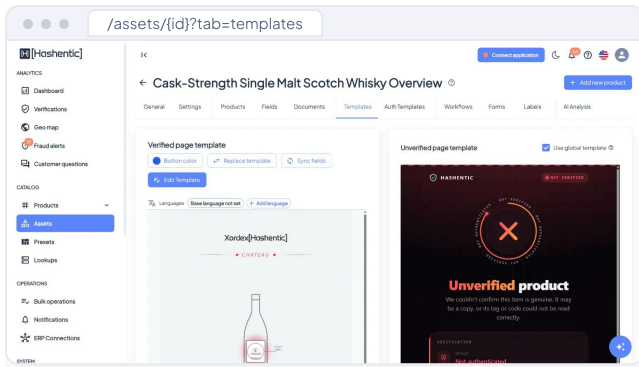
- ✓ **Button color:** color of the AI-assistant and documents buttons on the page; empty uses your brand color.
- ✓ **Unverified page template:** per asset, or **Use global template** from Settings; **failed page rules** can replace it for certain failures.
- ✓ **Sync fields:** refresh a template after you add or rename fields.
- ✓ **Auth templates:** alternative verified pages chosen per scan by tag type, product label or the scanner's country, for example a notice for scans outside your markets.



Auth templates. When several match a scan, the one highest in the list wins; drag rows to reorder.

Languages

Every page template can have versions in other languages: the asset's verified and unverified pages, each auth template, each failed page rule and the global unverified page in Settings. Visitors see the language their browser prefers. If there is no version in that language, they see the base content.



Languages under the verified page template: the base language and **Add language**.

Add a language

Language of the base content
English (en)

The language the current template is written in

New language
German (de)

Pick from the list or type a code such as pt-BR

☐ Copy the base content and translate it myself

☒ Translate with AI

Add Cancel

Add a language: the base language once, the new language, and copy or AI translation.

- The **Languages** bar under a template shows the base language and each version. **Add language** asks once for the **Language of the base content**, then for the **New language**: pick it from the list or type a code such as **pt-BR**.
- Copy the base content and translate it myself** starts from a copy. **Translate with AI** translates the texts and keeps the layout, images, links and placeholders; anything it could not translate stays as in the base content. AI translation is not available for templates that show an external website.
- Open a language to **Edit** it, refresh it with **Translate again with AI** (your edits to that language are replaced) or remove it with **Delete language**.
- Up to 10 languages per template. The button color is the same in every language.
- A regional browser language falls back to the language itself: a visitor with *pl-PL* sees the *pl* version, a visitor with *de-AT* the *de* version.

Translations start from the saved template

Save your changes before adding or retranslating a language. On auth templates and failed page rules, save the rule first. Later edits to the base content are not copied into the languages: update each language with **Translate again with AI** or by hand.

Failed page rules

The unverified page can change with the reason a scan failed, the type of tag or code, and the scanner's country. The **Failed page rules** sit below the auth templates on the asset's **Auth templates** tab; rules for all products are in System → Settings, under the global unverified page template.

A rule can look at three conditions:

- Failure reasons** ([Appendix A](#)):
 - Already scanned*: a one-time NFC link was opened again.
 - Blocked or withdrawn*: the product or this tag is blocked.
 - Internal use only*: the product line is limited to internal checks.
 - Authentication failed*: every other reason, such as an unknown code, a wrong signature or a counter mismatch.
- Authentication types**: the type of tag or code the link belongs to, known even for tags that were never registered.
- Countries**: from the scanner's internet address; needs the *Geolocation analytics* license feature.

New failed page rule [X]

Name *
Link already used

Conditions ⓘ

Failure reasons
Already scanned

Authentication types

Countries

Page template
+ Choose a template

Save the rule to add languages

New failed page rule: a name, the conditions and the page to show.

Working with rules:

- **New rule** asks for a **Name**, the **Conditions** and the **Page template**. All conditions must match; an empty condition matches everything (*Any failure, All*).
- The first matching rule wins: drag rows to change the order, and open a rule to change it.
- The page of each rule can have its own languages.
- Product labels are not offered: a failed scan cannot prove which product it belongs to.

A failed scan shows the first of these that applies:

- 1 The asset's failed page rules, first match.
- 2 The asset's own unverified page template.
- 3 The failed page rules in Settings, first match.
- 4 The unverified page template in Settings.
- 5 The built-in page, in the visitor's language.

With **Allow already verified asset page** turned on, repeat scans of secure tags keep showing the designed product page with a notice instead of a page for *Already scanned*.

13 Presets and lookups

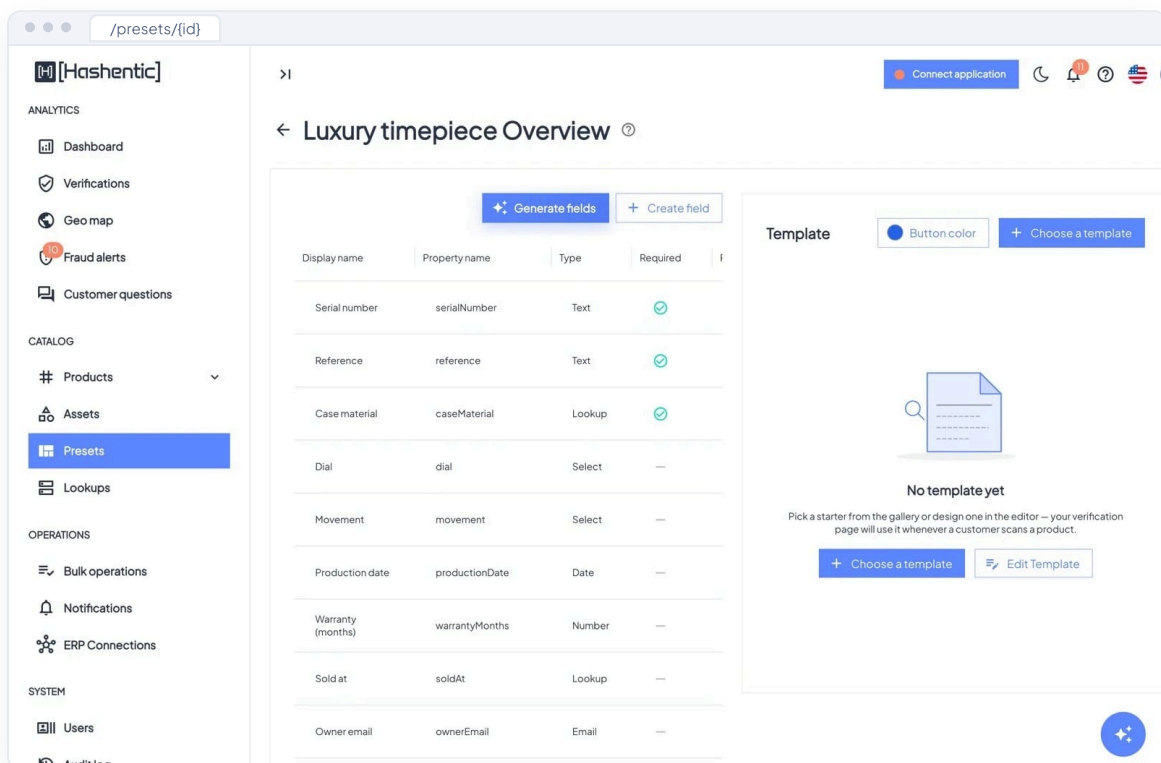
Two tools that keep a large catalog consistent: presets reuse a structure, lookups reuse values.

Presets

Menu Catalog → Presets

Permission Read / Write presets

A preset is a bundle of fields and a page template. Create one with **Create preset**, then add fields and choose a template exactly as on an asset. When you create an asset, choose the preset in **Use preset** and the asset starts with the same fields and page. System presets are provided by Hashentic; user presets are yours.



A preset for luxury watches: fields on the left, template on the right.

Lookups

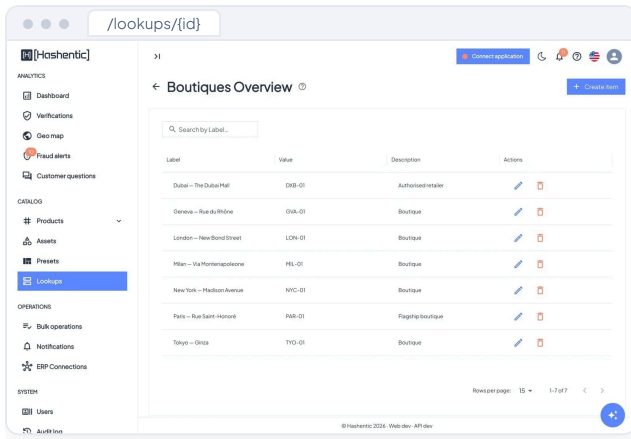
Menu Catalog → Lookups

Permission Read / Write lookups

A lookup is a named list, such as materials, boutiques or markets. Each item has a **Value** (stored on the product), a **Label** (shown to people) and a description.

Add items one by one (**Single mode**) or import a CSV or Excel file (**Multiple mode**), with the Bulk write license feature and the Write products permission, mapping its columns to value, label and description. Tick **Override** to replace the whole list.

Then use the lookup in any number of Lookup fields.



A **lookup** of boutiques: label, value and description of each item.

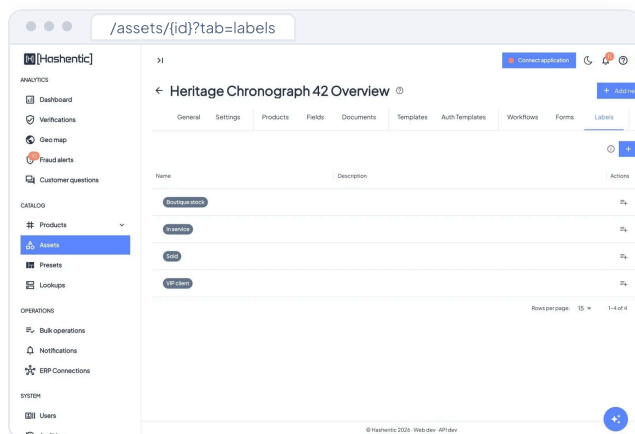
14 Labels and forms

Labels mark the state of products and tags; forms let customers send you information from the verification page.

Labels

Where Asset → Labels tab

Limit 15 labels per asset



Labels of the watch line.

Create labels with **New label** (name, color, description), for example *Boutique stock*, *Sold*, *In service*. Apply them on the product page, in bulk with **Bulk apply / remove**, or from workflows.

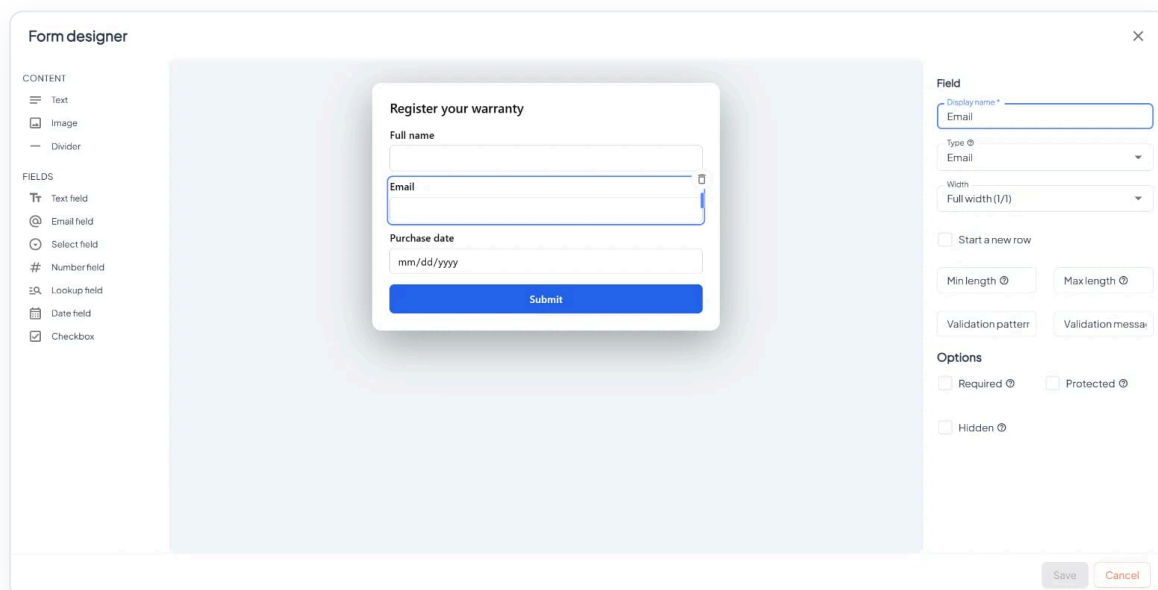
Labels can choose a different verification page (auth templates), decide which customers see a form, limit a workflow's scope, and filter product lists.

Forms

Where Asset → Forms tab

License Asset forms

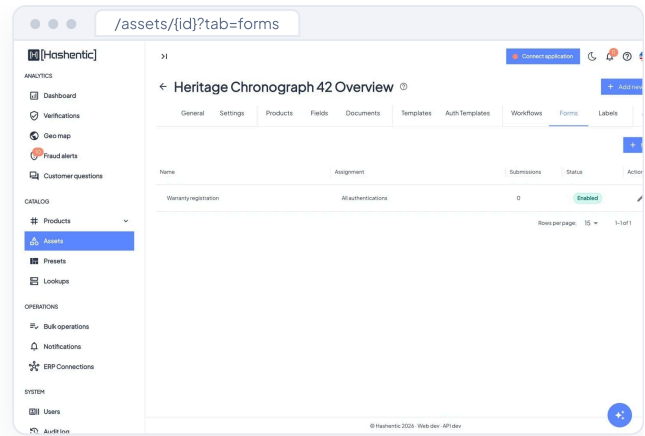
Forms appear on the verification page after a scan: warranty registration, newsletter sign-up, repair requests. **New form** opens the form designer with text, image and divider blocks, all field types and an optional GDPR consent checkbox.



Form designer. Blocks on the left, the live form in the middle, settings on the right.

- **Show this form to:** all authentications, a tag type, or products with a given label.
- **Allow only one submission per authentication** and **Allow the customer to skip this form.**

- **Show after delay (ms)** lets the page load first.
- **Submissions:** see every answer with product and date, and **Download submissions (CSV)**.
- A submission can start a workflow (trigger *On form submit*).



Forms tab with the warranty registration form.

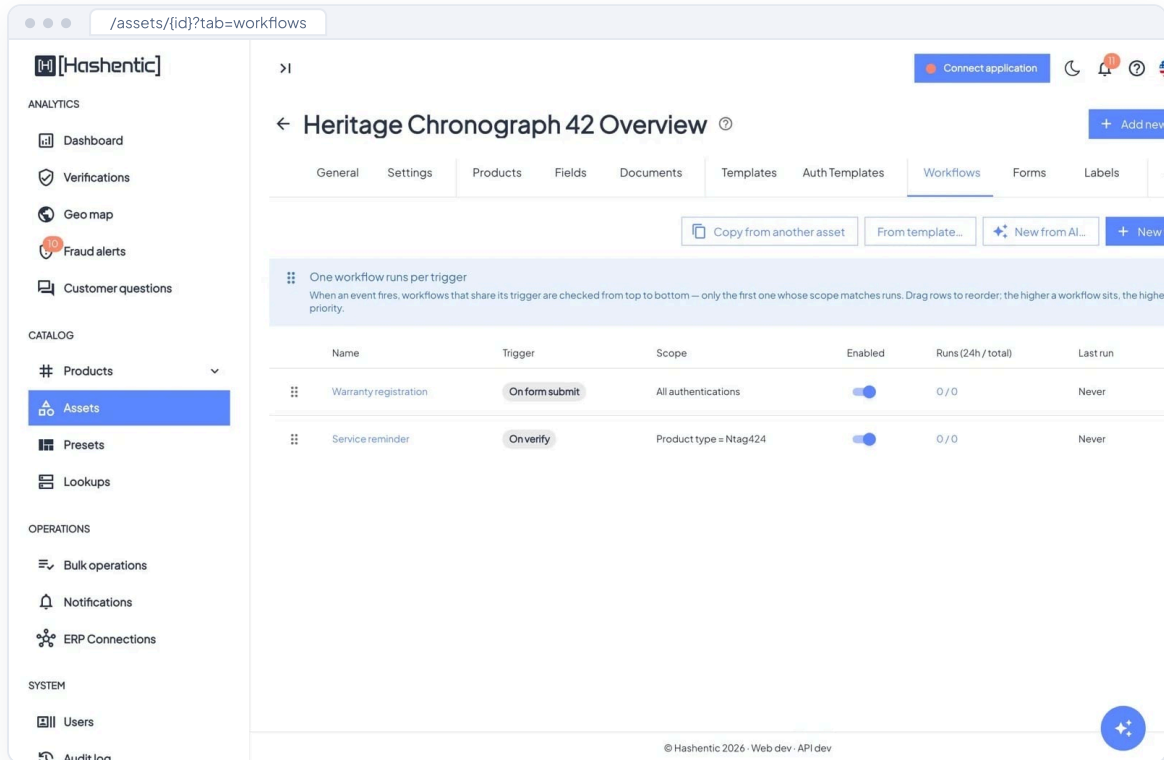
15 Workflows

Workflows react to what happens to your products, without anyone watching the screen: block a cloned tag, label a product when its warranty is registered, warn the team about repeated scans, or tell your CRM.

Where Asset → Workflows tab

Permission Read / Write workflows

License Workflows



Workflows of an asset. Trigger, scope, on/off switch, runs in the last 24 hours and in total, and the last run.

Building blocks

Triggers

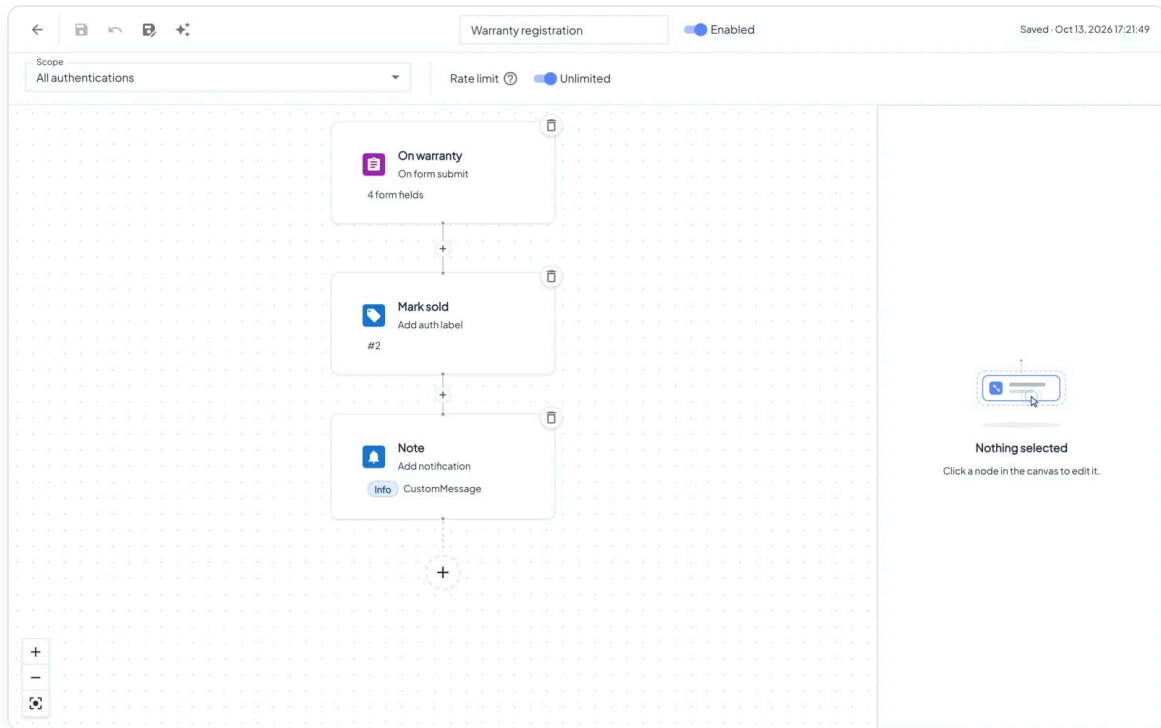
On verify (every genuine scan) · On form submit · On product blocked · On product create · On external webhook · On fraud detected (with a minimum severity).

Actions

Show form · Send mail · Block product · Block authentication · Update custom fields · Add notification · Add label · Add auth label · HTTP request.

Logic

Condition with AND/OR groups on fields, country, OS, tag type, scan counts, distance from the last scan, time of day, product age or labels, with then/else branches. Delay waits minutes, hours or days.



The workflow editor. The canvas shows the trigger and steps; use **+** on a connection to insert a step. Click a step to edit it in the panel on the right.

Good to know

- **One workflow runs per trigger.** If several workflows of an asset share a trigger, the first one (top of the list) whose **scope** matches runs. Drag rows to set the order.
- **Scope** limits a workflow to a tag type or category, a field value, specific tags, or tags with a label.
- Every save creates a new **version**; you can view and restore earlier ones.
- Start from **From template...** (for example *Anti-counterfeit: block on second scan*), copy from another asset, or describe the workflow to **New from AI...**
- In text fields, the **token picker** inserts values such as the scan's country, the product ID or a custom field.

Runs — Repeat scan check

[Add filter](#)

ID	Started	Status	Trigger	Product	Duration	Current step	Actions
8	Oct 13, 2024 17:21:52	Completed	On verify	45suQCD	4.8s	—	ⓘ
7	Oct 13, 2024 17:21:52	Completed	On verify	D4EH5ow	4.8s	—	ⓘ
6	Oct 13, 2024 17:21:52	Completed	On verify	3WpFAST	4.9s	—	ⓘ
5	Oct 13, 2024 17:21:52	Completed	On verify	4BQq5m	4.9s	—	ⓘ
4	Oct 13, 2024 17:21:52	Completed	On verify	8YEWnJT	4.9s	—	ⓘ
3	Oct 13, 2024 17:21:52	Completed	On verify	BZ2Pme	4.8s	—	ⓘ
2	Oct 13, 2024 17:21:52	Completed	On verify	BZ2Pme	4.9s	—	ⓘ

Rows per page: 15 1-7 of 7

Runs: open them from the runs count. Each run shows its status, product and every step's result.

i Connecting other systems

A workflow with the **On external webhook** trigger gets its own URL and secret: your system signs each request with the secret, and Hashentic starts the workflow for the product named in the payload. **HTTP request** steps call your systems; their addresses must be listed in **Settings** → **Workflows URL allowlist**. The **Integration guide** in the menu explains both.

16 Writing tags and printing barcodes

Creating products and giving them their authentication happens in one dialog: **Products** → **Add new**. NFC tags are written through a USB reader connected with the Desktop utility; barcodes are generated instantly and exported for printing.

Menu Catalog → Products → Add new

Permission Write products

License Bulk write for Multiple mode

Add product, NFC tag, Single mode. The header button shows whether the Desktop utility is connected.

Choose what to create

- **NFC Tag**: writes the tag on the reader. The admin panel shows the type of the tag on the reader (NTAG 424, NTAG 215, EM4425).
- **Barcode**: creates a product with a QR/barcode authentication; no hardware needed.
- **Without authentication**: creates the product only; add a tag or code later on its page.

Single mode

Choose an asset → **Place tag / Fill values** → **Write**. Pick the asset in **Asset name**, fill in its fields, and click **Write** (or **Create**). When the tag is written, the product page opens.

Barcode, Single mode: the asset's fields to fill in.

Multiple mode: create many products from a file, a count or an ERP.

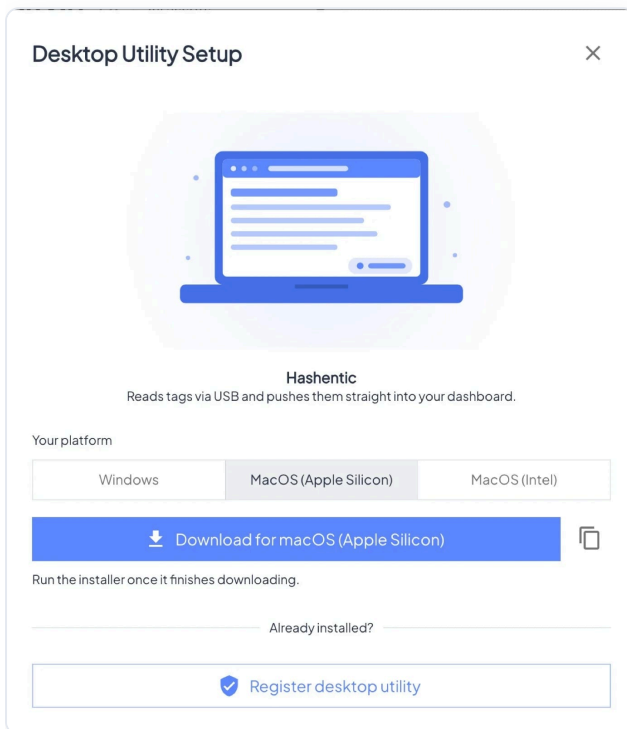
Multiple mode

Choose an asset → **Set up fields** → **Write tags / Generate barcodes**.

- ✓ **Upload file**: CSV, XLSX or XLS, up to 100,000 rows and 10 MB. The first row holds the column names.
- ✓ **From ERP**: fetch records from a saved ERP connection ([chapter 17](#)).
- ✓ Rows that fail validation are highlighted; fix them with the edit icon before you start.
- ✓ **NFC tags** are written one after another: place a tag, wait for "written", take it off, place the next. Keep **Save import** ticked to resume an interrupted session later.

- ✓ **Generate by number:** just a count, up to 50,000, for assets without required fields.
- ✓ **Set up fields** maps each asset field to a column. Columns named exactly like a field's property name are mapped automatically.
- ✓ **Barcodes** are generated in the background as a [bulk operation](#); you can close the page.
- ✓ Tick **Confirm on tag override** to be asked before a tag that already holds data is rewritten.

The Desktop utility



Desktop Utility Setup, from the menu (**Setup desktop utility**) or **System** → **Applications**.

The Desktop utility is a small app for **Windows** and **macOS** (Apple Silicon and Intel) that connects a USB NFC reader to your browser session. It runs in the system tray and offers updates when they are available.

- 1 Download it from the setup dialog and install it.
- 2 Click **Register desktop utility**: the app opens and signs in as you. Alternatively paste the **Desktop application token** from **System** → **Applications**.
- 3 Plug in the reader. When the utility is signed in, the header button turns green: **Connected**; the Add product dialog shows whether the reader itself is connected.

The utility must be signed in with the same account as the browser. The header button states are *Connect frontend* (browser not connected), *Connect application* (utility not running or not signed in) and *Connected*.

Exporting barcodes

Open **Download** on a product, **Download barcodes** on an asset's Products tab (exports everything matching the filters) or on a finished bulk operation.

- **Format:** PDF (print-ready A4 sheets) or CSV, XLSX, TXT lists of links.
- **Barcode type:** QR code, DataMatrix or Code 128; optionally with your logo in the center of the QR code.
- **URL version:** *Public* (your verification address), *Internal*, and for GS1 assets *GS1 Digital Link* and *GS1 barcode*.
- **Size:** five presets from Extra small to Extra large, or a custom size with readability hints.
- **Caption settings:** print a field value or your own text under each code.
- **Fixed settings:** pages, codes per page and grid of the resulting sheet.

Export

Barcode Settings | Caption Settings | Fixed Settings

Format ⓘ

PDF CSV XLSX TXT

Barcode type ⓘ

QRCode

☒ Include center logo ⓘ

Filename ⓘ

barcodes.pdf

Clone count ⓘ

1

Number of identical copies of this barcode to include in the export.

URL version ⓘ

Public Internal GSI Digital Link GSI barcode

Generate PDF Cancel

Export: format, symbology, URL version and size.

Updating products

Update product

Connect application

Single Mode | Multiple Mode

1 Scan product 2 Manage product

Device

LISTENING ON Webcam - QR NFC reader - Tag

Webcam preview

Show a QR or tap a tag.

Not supported

Update product: scan with a webcam or the NFC reader.

Products → **Update** finds products by scanning them: show the QR code to your webcam or tap the tag on the reader.

- **Single mode** opens the scanned product's page, ready to edit.
- **Multiple mode** collects many products (by scanning, from the mobile app's scan queue, or by a query on the asset), lets you set shared values with per-item overrides, and runs the update in the background.

Only fields with the *Update* stage can be changed after creation. Editing needs the Update records license feature.

17 Bulk operations and ERP

Large jobs run in the background and are tracked here. ERP connections bring product data straight from your systems into the tag-writing wizard.

Bulk operations

Menu Operations → Bulk operations

Permission Read / Write bulk operations

License Bulk write

Bulk operations: barcode generation runs and bulk updates, with status, progress, duration and who started them.

Operation details: every item and its status; switch on **Failed only** to see what needs fixing.

- **Statuses:** Pending, Running, Completed, Completed with errors, Failed, Cancelled.
- **View details** lists the items. Edit a failed row and retry it, or use **Retry failed** for all.
- **Download barcodes** exports the codes of a finished barcode run.
- **Cancel** stops a running operation; items already done are kept.

ERP connections

Menu Operations → ERP Connections

Permission Manage ERP connections

License Bulk write

Save a reusable, read-only connection to your ERP or product database:

New connection

×

Connection name

Source type ⓘ
REST / JSON

URL ⓘ

Method ⓘ
GET

Records JSON path ⓘ

Authentication ⓘ
None

Custom headers ⓘ
+ Add header

Cancel

Save

New connection to a REST/JSON source.

- **REST / JSON, JSON-RPC** and **GraphQL** APIs, with no authentication, a bearer token, basic authentication or an API-key header, plus custom headers.
- **SQL databases:** PostgreSQL, SQL Server, Oracle, MySQL/MariaDB, with a single read-only query.
- **MongoDB**, with a collection, filter and projection.

Secrets are stored encrypted and shown masked. Each connection belongs to the person who created it. Use it in **Add new** → **Multiple mode** → **From ERP**: **Test / preview** shows the first 50 records, **Fetch records** loads up to 100,000.

For security, connections to local or private-network addresses are refused.

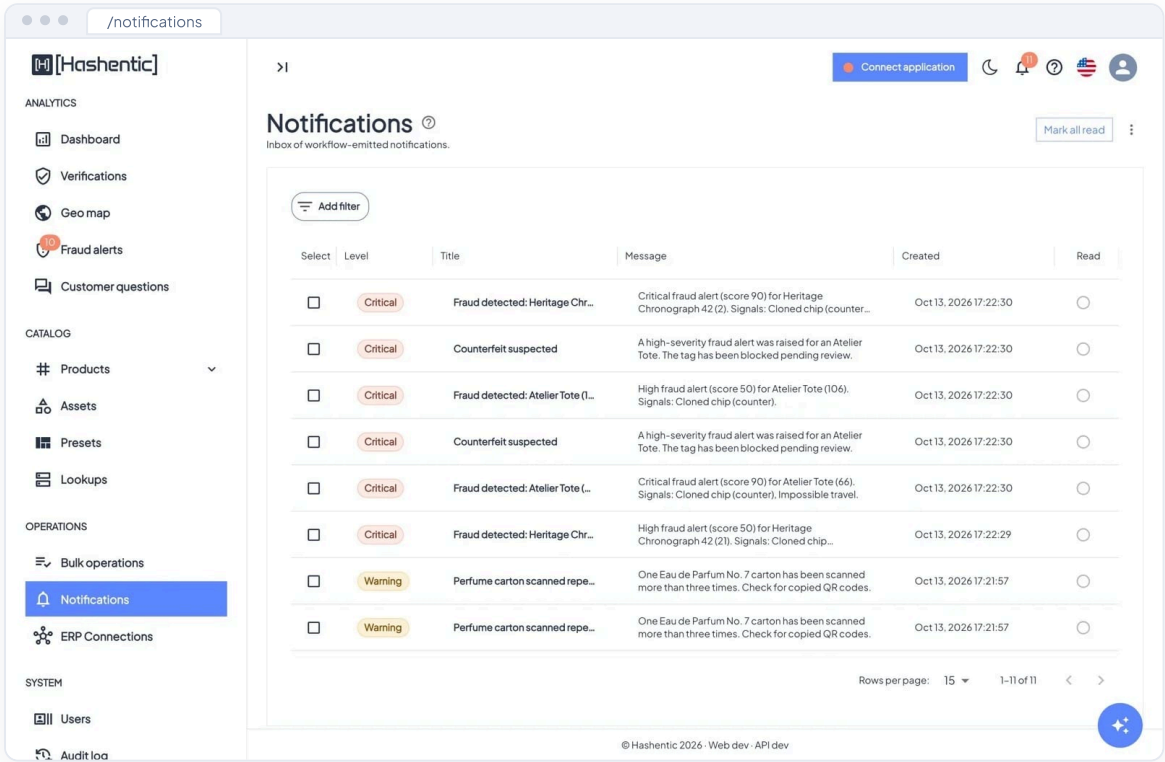
18 Notifications and audit log

Notifications tell you what needs attention; the audit log records who did what.

Notifications

Menu Operations → Notifications, and the bell in the header

Permission Read notifications



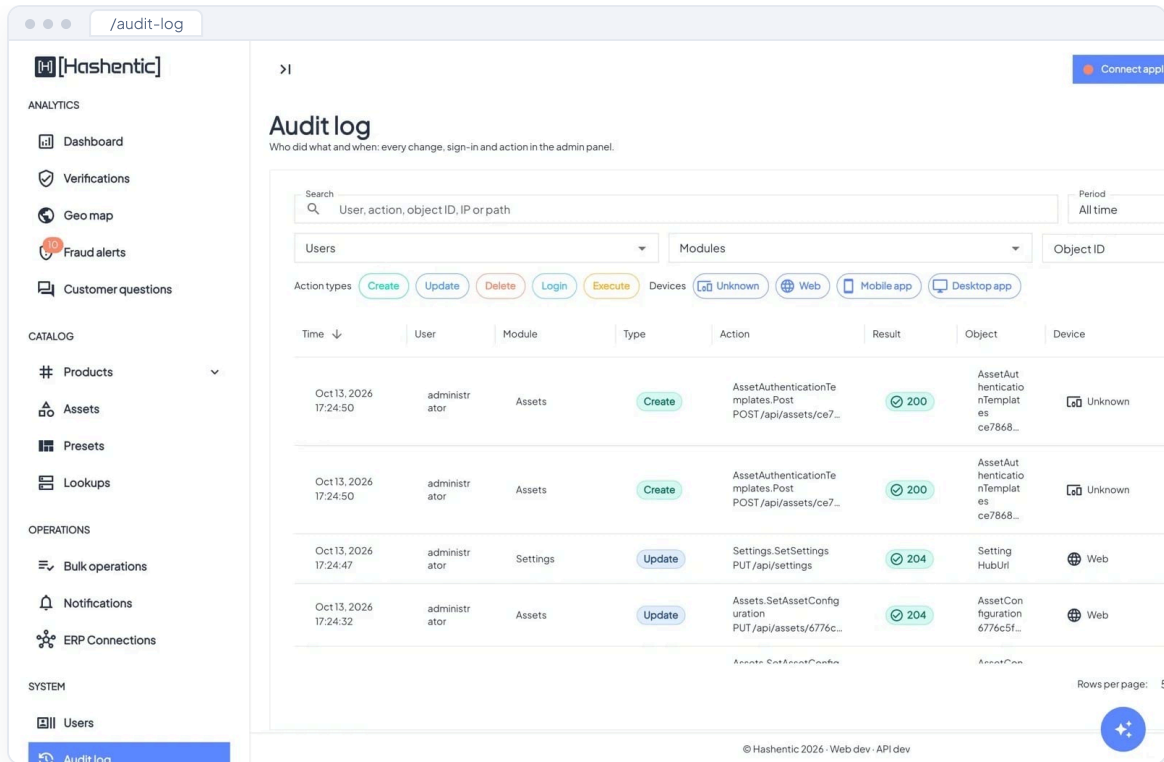
Notifications from the fraud engine and from workflows, by level: Info, Warning, Critical.

- ✓ System notifications: *Fraud detected* (High and Critical alerts), *Counterfeit anomaly* (a burst of failed scans), *High verification count* and *License expires in N days*.
- ✓ Filter by **Unread only** and date; mark read, or select and delete.
- ✓ Workflow notifications with your own title and text.
- ✓ Open a notification to see its details, the product, and the workflow run that sent it.

Audit log

Menu System → Audit log

Access Super User only



Audit log: every change, sign-in and action, from the web, the mobile app and the Desktop utility.

Filter by period, users, modules (Users, Settings, Assets, Products, Workflows, License, AI...), action type (Create, Update, Delete, Login, Execute), device and result. Open an entry to see the exact changes (old → new values), then jump to

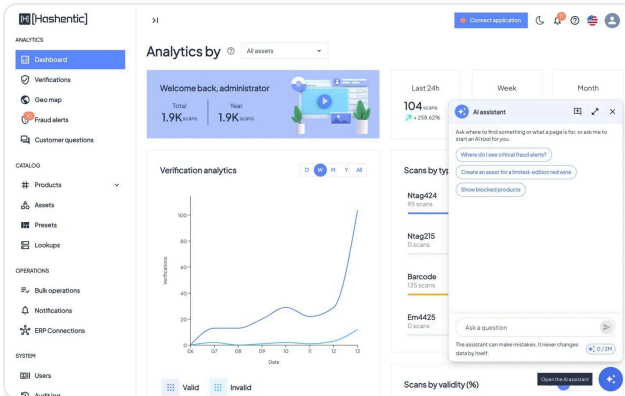
Show all activity of this user or **Show history of this object**.

19 AI features

AI helps in four places: it answers your customers, answers you, analyzes your scan data, and drafts configuration for you. It never changes data on its own.

Settings AI analysis, the AI assistant and customer answers are switched on in Settings

License AI, plus AI assistant / AI analysis / Customer AI



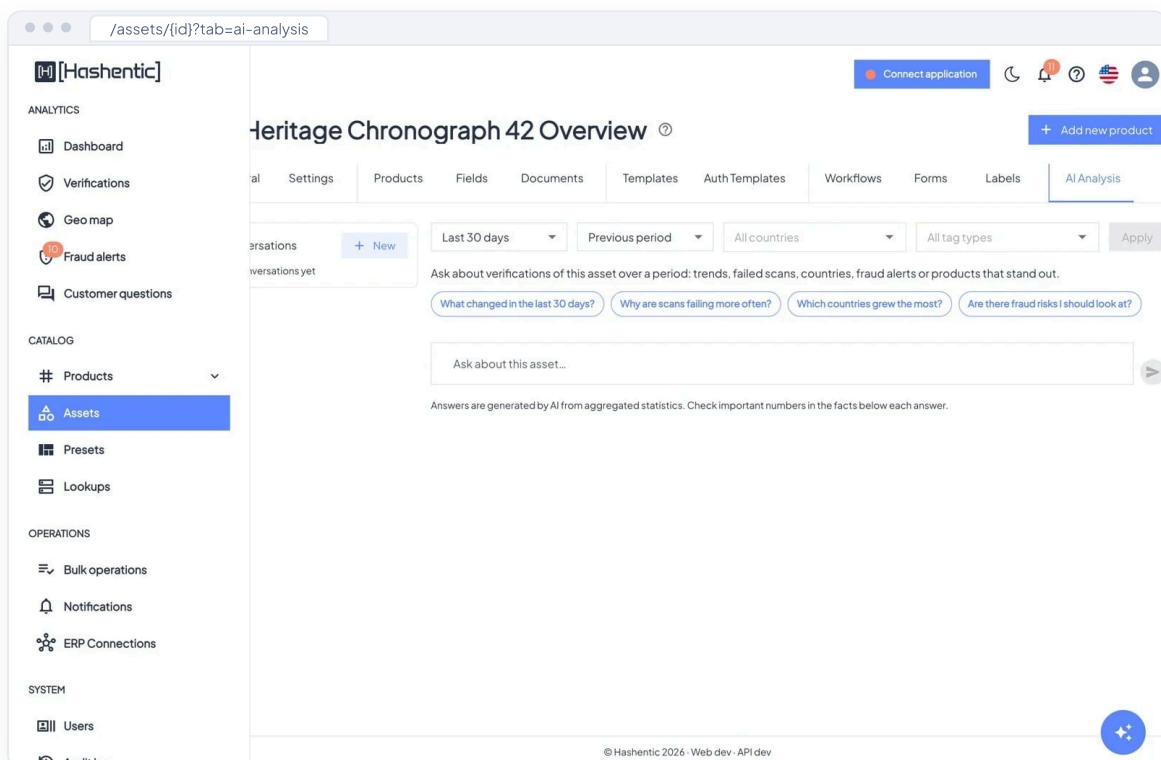
AI assistant, opened with the sparkle button.

AI assistant

Ask where something is or how to do it: "Where do I see critical fraud alerts?", "Show blocked products", "Make a workflow that emails me about failed scans". Answers come with buttons that open the right page or start an AI tool. On an asset or product page, the assistant also uses that line's documents.

AI analysis

The **AI analysis** tab on assets and products answers questions about your scans ("Why are scans failing more often?", "Which countries grew the most?") with findings, recommendations, a chart and the figures it used. Only aggregated counts, dates, country codes, rounded locations and product labels are sent to the AI service; IP addresses, browser details, form answers and owner data never are.



AI analysis with period, comparison, country and tag-type filters, and suggested questions.

Answers for customers

The assistant on the verification page answers in the customer's language from public fields, passport data and public documents. See [Customer questions](#).

Generators

Create an asset from a description, generate fields, generate a page template, get protection recommendations, and draft or modify workflows.

Documents: what the AI knows

Upload manuals, care instructions, warranty terms and certificates (PDF, DOCX, TXT or Markdown) at three levels: **Settings** → **Brand documents** for the whole brand, the asset's **Documents** tab for a product line, and the product's **Documents** tab for one item. Set each document's **Audience**:

- ✓ **Internal only** (default): used by the AI assistant and analysis for your team.
- ✓ **Public**: downloadable from the verification page, used for customer answers, and can get a permanent public link.
- ✓ **Authorities, Recyclers, Repairers**: for Digital Product Passport partners.
- ✓ Each document is indexed for AI; the status chip shows when it is *Indexed* and ready.

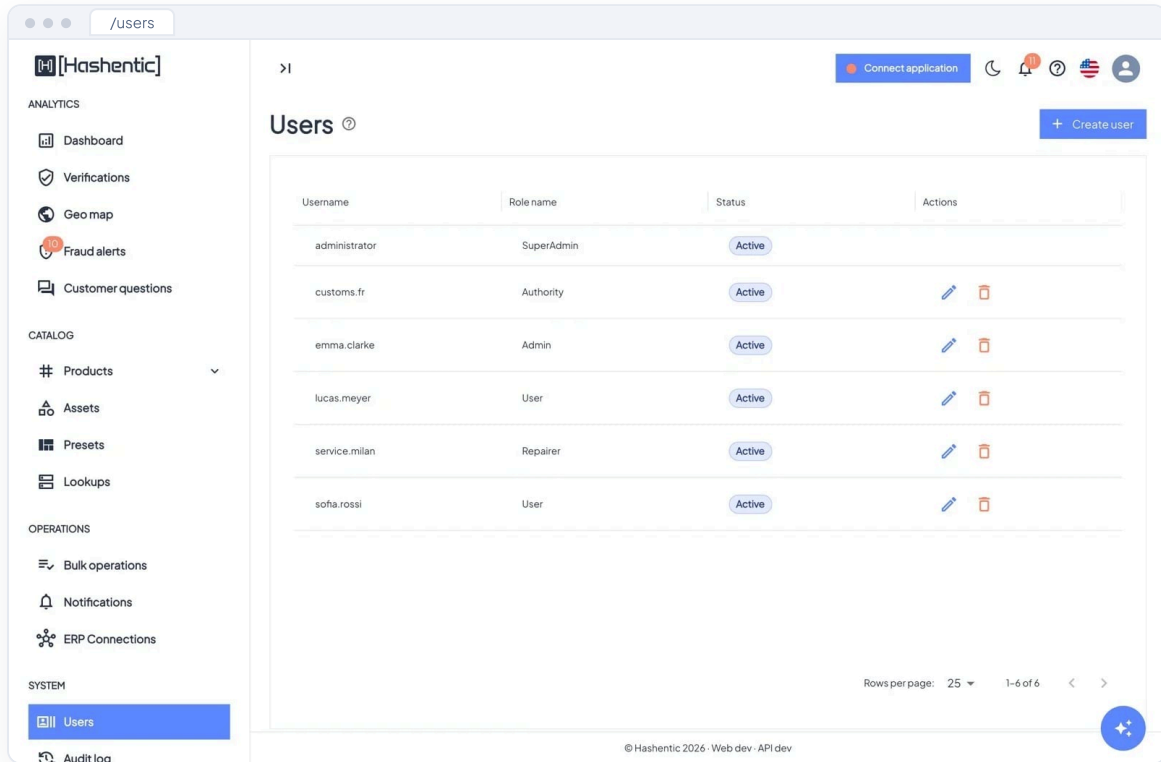
20 Users and access

Give each person their own account, with exactly the permissions and product lines their job needs.

Menu System → Users

Permission Read / Write users

Limit number of users in your license



Users with their role and status. The pencil edits an account, the bin deletes it.

Edit account: details, status and permissions.

Create user asks for:

- **Username and Email.**
- **Role:** Admin, User, or a partner role (Authority, Recycler, Repairer). Permissions that come with the role are ticked and cannot be removed.
- **Password:** at least 12 characters with a letter and a digit. You set it and pass it on; no invitation email is sent.
- **Status:** Active users can sign in; Inactive users keep their data but cannot.
- **Permissions**, grouped by area.
- **Allowed assets** for roles that do not see everything.

To reset someone's password, type a new one when editing the account; this also signs them out. Nobody can give out a higher role or permissions they do not have themselves.

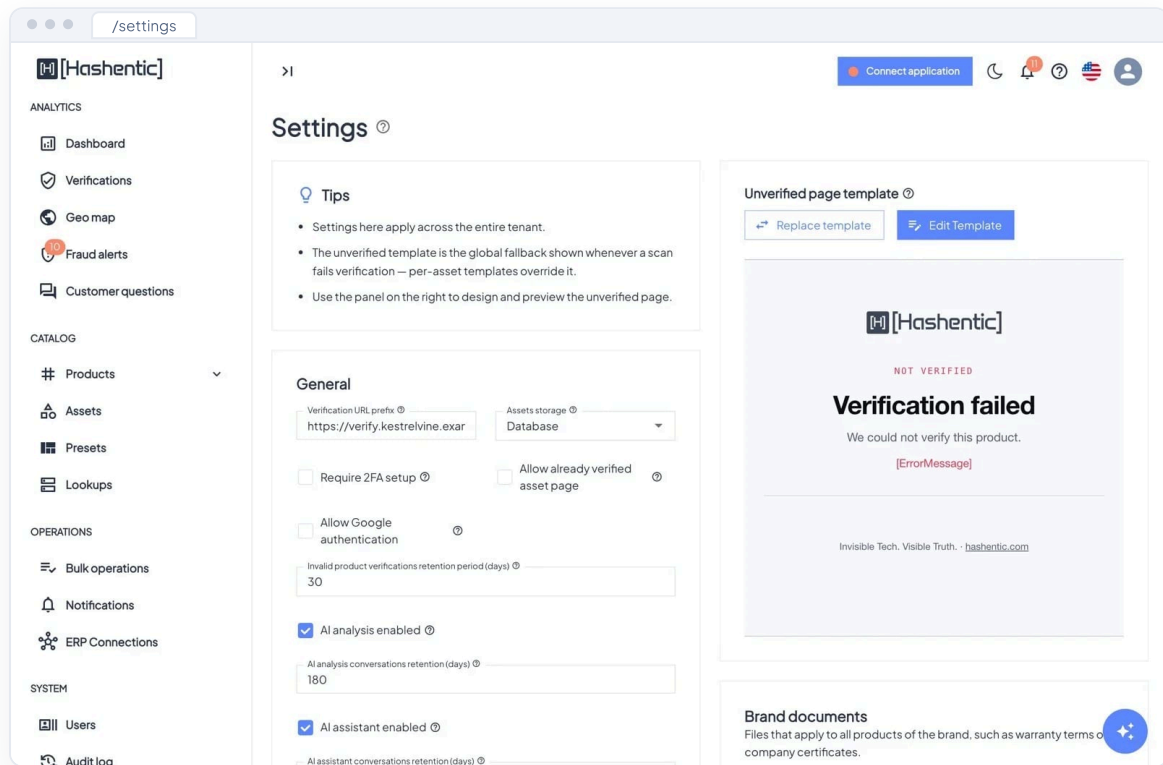
21 Settings, branding and license

Workspace-wide configuration: how verification links look, security rules, AI switches, fraud sensitivity, your brand identity and your license.

Settings

Menu System → Settings

Permission Read / Write settings



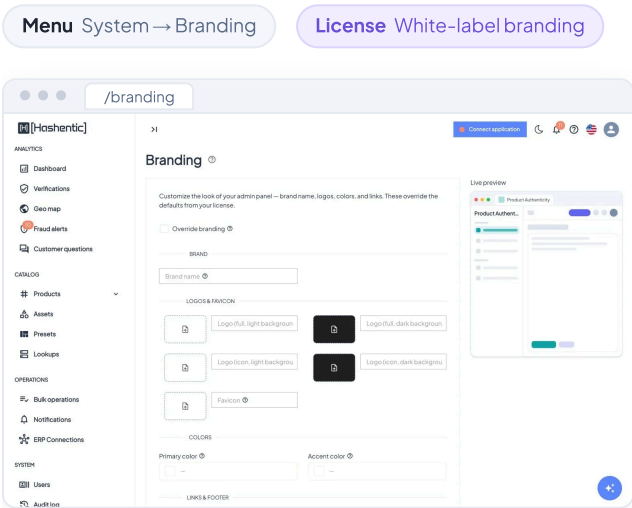
Settings. General settings on the left; the global unverified page, brand documents and the workflows URL allowlist on the right.

Setting	What it controls
Verification URL prefix	The public address at the start of every verification link and QR code, such as <code>https://verify.your-brand.com/v</code> . Must use https.
Default NTAG 424 key	The key written into new NTAG 424 tags. Changing it affects only tags written afterwards.
Assets storage	Where integrity records are kept: Database or Blockchain. Fixed once the first asset or product exists.
Require 2FA setup	Every user must set up two-factor authentication at sign-in and cannot turn it off.
Allow Google authentication	Existing users can sign in with the Google account that matches their email.
Allow already verified asset page	Show the designed product page on repeat scans of secure tags. When on, it applies to every asset; when off, each asset can still turn it on.
AI analysis / AI assistant enabled · Answer customer questions on the verification page	Switch the AI features on, with retention periods and a daily limit for customer questions.
Maximum document file size (MB)	Upload limit for documents, 1–25 MB (default 10).

Setting	What it controls
Invalid product verifications retention period (days)	How long failed scans are kept (default 30).
Verification alerts	A Critical notification when a product has more failed scans in an hour than the threshold (default 5), and a Warning when a single tag reaches a scan count (default 1,000).
Fraud & anomaly detection	On/off and every threshold of the fraud engine: travel speed and distance, velocity window and count, gray-market scans and window, invalid-burst window, alert cooldown, High and Critical score cutoffs.

On the right of the page you also design the **Unverified page template** (shown for failed scans of assets without their own) with its languages, add **Failed page rules** that pick a different failed page for all products by failure reason, tag type or country ([Verification page templates](#)), manage **Brand documents** for AI answers, and maintain the **Workflows URL allowlist** of addresses workflows may call.

Branding



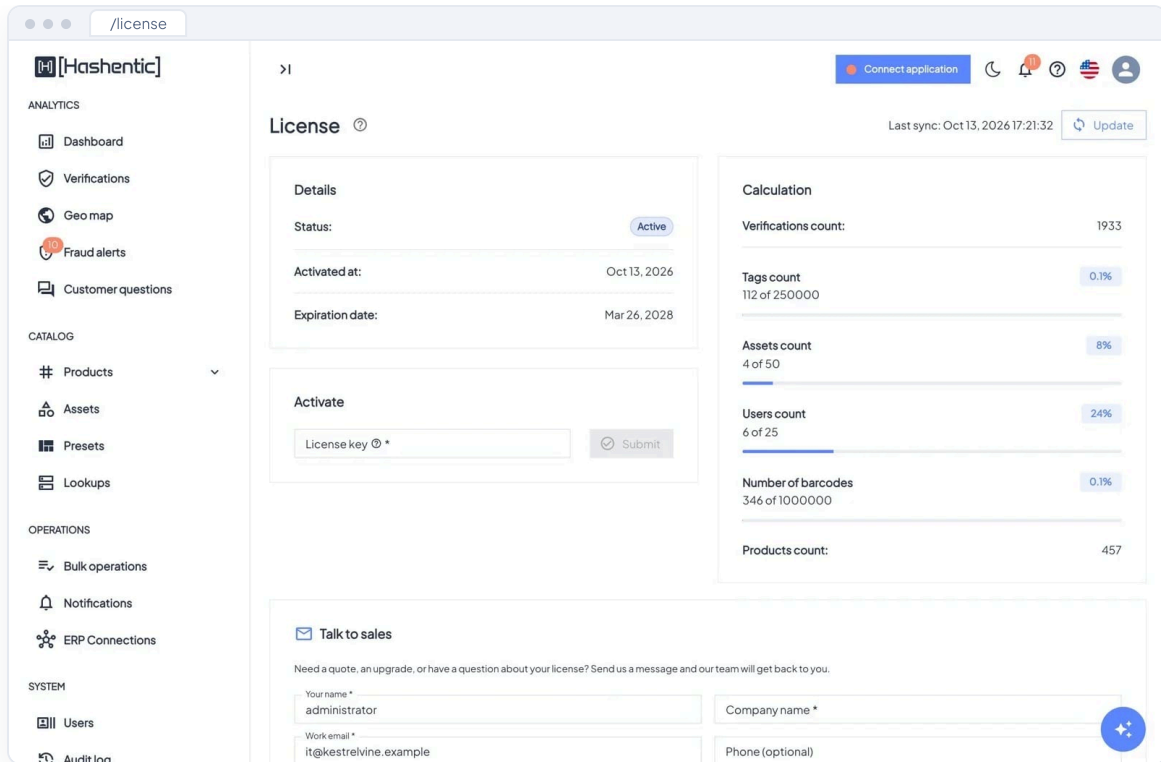
Branding with a live preview on the right.

Turn on **Override branding** to replace the defaults of your license with your own:

- **Brand name**, shown in the admin panel, page titles and verification pages.
- **Logos** (full and icon, for light and dark backgrounds) and a **favicon**. The icon logo is also embedded in QR codes.
- **Primary and accent colors**.
- **Links**: website, support, privacy policy, terms; **footer** and "Powered by" text on verification pages.

License

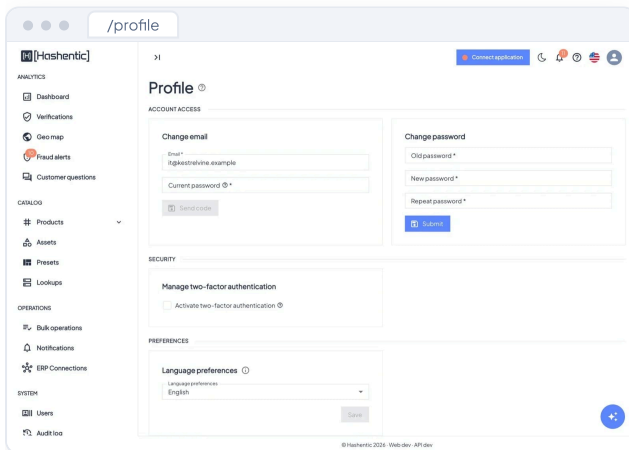




License. Status and dates, usage against your limits, activation and a contact form.

- ✓ **Details:** status (Active, Expired, Blocked, Stale, Inactive), activation and expiry dates.
- ✓ **Activate:** paste a license key (format XXXX-XXXX-XXXX-XXXX-XXXX). Activation links from email are applied automatically after sign-in.
- ✓ **Calculation:** verifications, tags, assets, users, barcodes and products, with progress bars against your limits.
- ✓ **Update** fetches the latest version of your license; **Talk to sales** sends a message to the Hashentic team.

Your profile



Profile, from the avatar in the header.

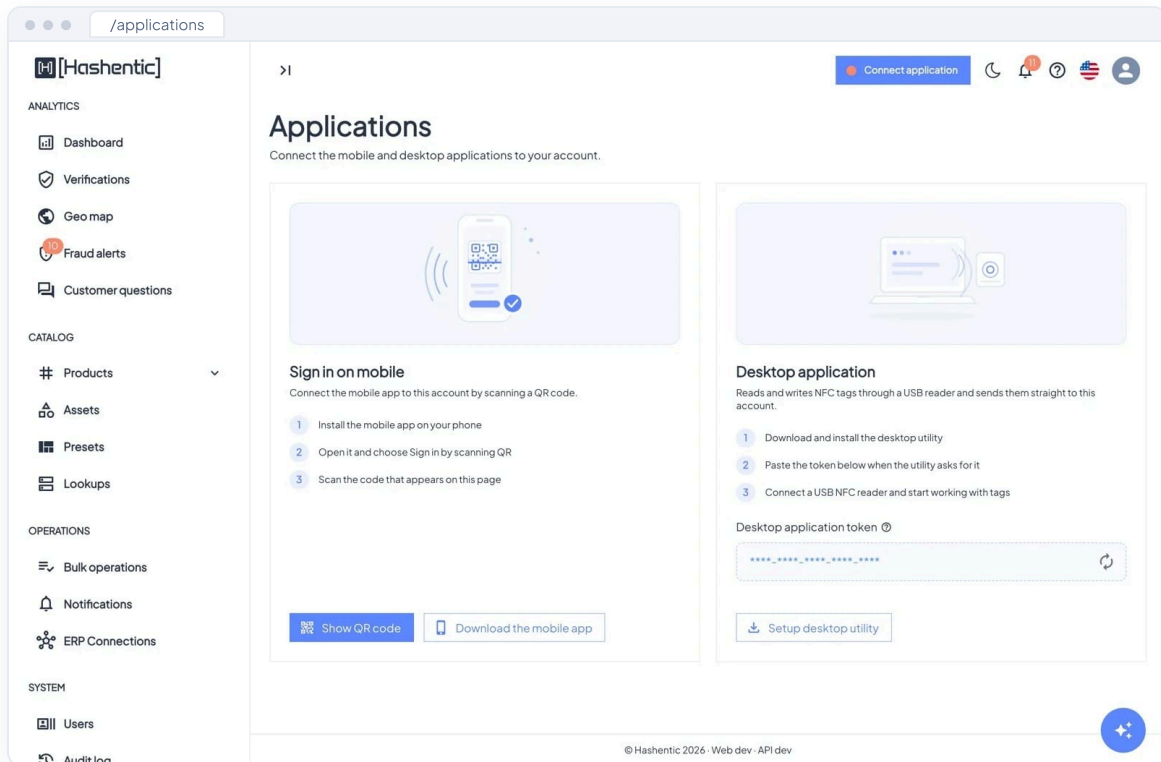
- **Account access:** change your email (confirmed with a code sent to the new address) and your password.
- **Security:** **Activate two-factor authentication** with any authenticator app, and manage your 10 one-time recovery codes.
- **Preferences:** your language for the admin panel and for emails.

22 Mobile app and Desktop utility

Two companion apps take Hashentic away from the desk: the mobile app for staff in stores, warehouses and service centers, and the Desktop utility for writing NFC tags on the production line.

Menu System → Applications

License Mobile applications for the mobile app



Applications. Sign in on mobile with a QR code, download the apps, and get your Desktop application token.

The mobile app

Available for **Android** 8.0 and later and for **iPhone** with iOS 16.4 and later. Reading and writing tags needs a phone with NFC. The app follows the phone's language (English or Russian) and supports light and dark themes.

For everyone

- **Is it genuine?** Anyone can check a product without an account: scan the QR code, tap **Read NFC tag**, or type the link. The app checks that the link belongs to a registered Hashentic workspace before opening the brand's page.

For staff

- **Sign in** with your workspace address, username and password, or by scanning the QR code from **Applications** → **Sign in on mobile**. Two-factor authentication is supported, and you can keep several accounts.
- **App lock** with a 6-digit PIN and/or Face ID or fingerprint.
- **Scan** a product to see a green *Verified* or red *Verification failed* result with the reason and public fields, then open the product or **Save for batch update**.
- **Products:** search by identifier or tag UID, filter by asset, label, tag type and status, and open the product card with its tags, fields and history.
- **Create** products and **edit** fields (secure tags may ask you to tap the tag first).
- **Write NFC tags** (NTAG 424, NTAG 215, EM4425) straight from the phone, with cryptographic read-back. Interrupted writes can be finished or discarded later.
- **Block, unblock or delete** products, according to your permissions.
- **Open a product from the web:** scan the **QR for the mobile app** shown on a product page.
- Partner roles (Authority, Recycler, Repairer) see and edit only the passport fields meant for them.

The Desktop utility

A small Windows and macOS app that connects a USB NFC reader to your account; you keep working in the browser. Download it from **Setup desktop utility**, sign in with **Register desktop utility** or the **Desktop application token**, and plug in the reader. It runs in the background from the system tray and shows which account it is connected to. When a new version is available it offers the update and installs it once it is idle, not in the middle of writing a tag. See [chapter 16](#) for writing tags with it.

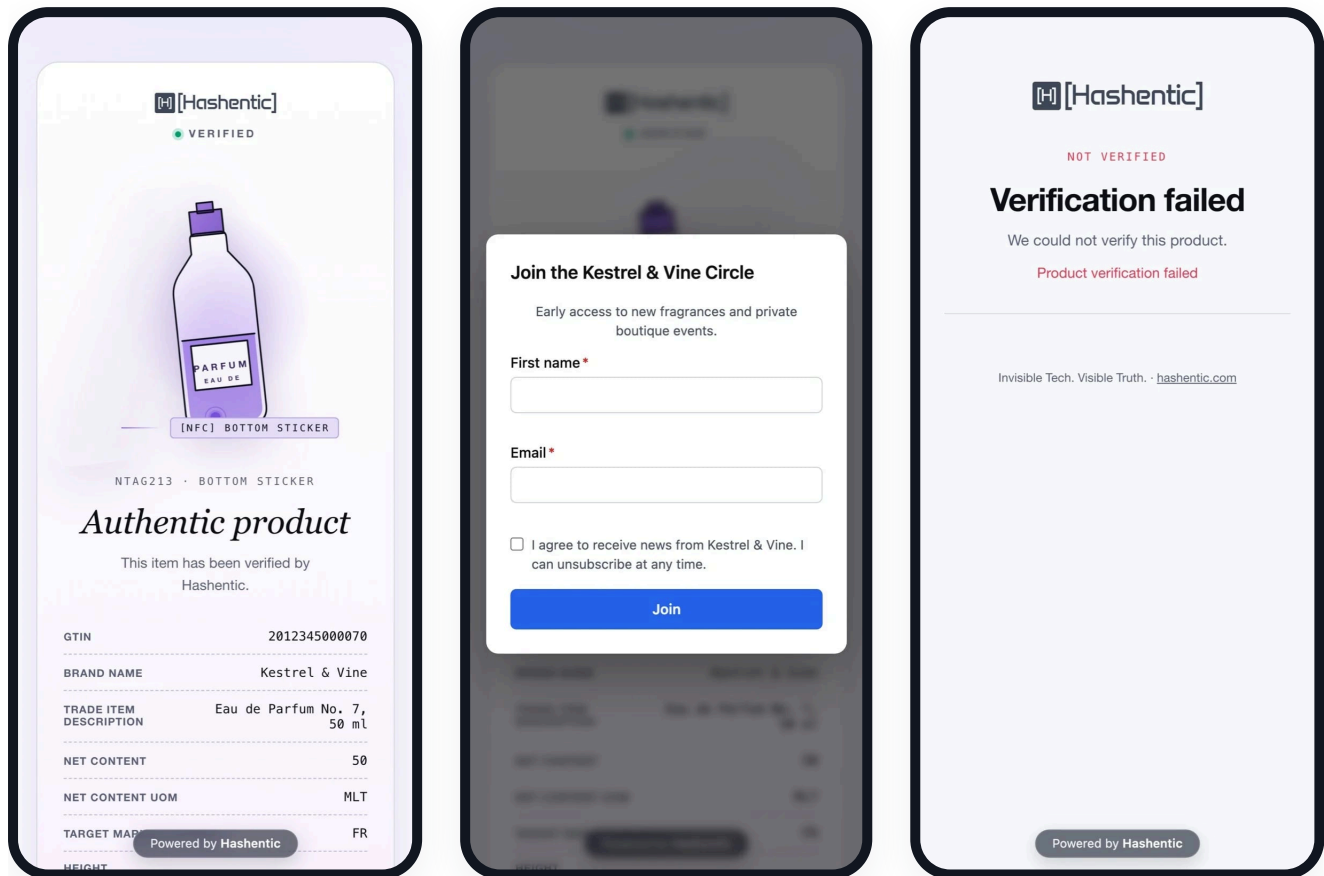


Tokens

The Desktop application token on the Applications page signs the utility in as you. **Regenerate** invalidates the old token, which signs out any utility still using it.

23 The consumer verification page

What your customer experiences after tapping the tag or scanning the code: an instant answer, in your brand's design, and a reason to stay.



Verified. The Cosmetics design from the gallery with the product's fields.

A form offered after the scan, here a newsletter sign-up with consent.

Not verified. Shown for failed scans; design it in Settings or per asset.

What happens on a scan

- 1 The tag or code opens your verification link. A secure NFC tag adds a one-time cryptographic code to it.
- 2 Hashentic checks the product, the tag and its counter, and records the scan with time, location and device.
- 3 The customer sees the asset's **verified** page, or an **auth template** that matches the scan's tag type, label or country. Failed scans show the **unverified** page, or the page of a **failed page rule** that matches the failure reason, tag type or country. A page with several languages opens in the language of the visitor's browser.
- 4 Workflows with the *On verify* trigger run, and fraud detection takes the scan into account.

On the page

- ✓ **Your design** from the gallery, the block builder, your own HTML or your website.
- ✓ **Your customer's language:** templates you translated open in the visitor's browser language; the built-in page speaks the six admin panel languages.
- ✓ **Ask about this product:** the AI assistant answers in the customer's language, using only public information. It never confirms authenticity itself; that is the scan's job.
- ✓ **Bot protection** (Cloudflare Turnstile or Google reCAPTCHA) guards the AI assistant and forms, never the verification itself.

- ✓ **Documents** button: downloads of the public manuals and certificates for the product.
- ✓ **Forms**: warranty registration, sign-ups, repair requests, with consent checkboxes linked to your privacy policy and terms.
- ✓ The assistant and forms work in English, German, Spanish, Polish, Russian and Chinese, following the visitor's browser.

! **Repeat scans of secure tags**

Each tap of an NTAG 424 DNA or EM4425 tag produces a new code. Opening the same link a second time (from browser history or a shared message) fails as "Already verified". That protects against copied links. If customers like to come back to the page, turn on **Allow already verified asset page**: designed pages are then shown again with the notice "Product is not verified. Current url used more than once." (without documents, assistant or forms).



Step-by-step guides

Short recipes for the jobs you will do most often, from securing your account to answering a counterfeit alert. Each one names the exact buttons to click.

24 Secure your account

25 Set up a new product line

26 Design the verification page

27 Translate the verification page

28 Show a different page when a scan fails

29 Create QR-coded products and print labels

30 Write NFC tags with the Desktop utility

31 Investigate a fraud alert

32 Block cloned tags automatically

33 Collect warranty registrations

34 Add a team member

35 Update many products at once

36 Help the AI answer your customers

37 Connect the mobile app

24 Secure your account

Turn on two-factor authentication so a stolen password is not enough to get into your account. It takes two minutes and an authenticator app such as Google Authenticator or Microsoft Authenticator.

- 1 Click your avatar in the top-right corner, then **Open profile**.
- 2 Under **Security**, tick **Activate two-factor authentication**.
- 3 Scan the QR code with your authenticator app, or type the code shown under it into the app.
- 4 Enter the 6-digit code from the app in **Two-factor authentication code**, your **Account password**, and click **Send**.
- 5 Save your 10 **recovery codes** with **Copy all** or **Download .txt**, keep them somewhere safe, tick **I have saved my recovery codes** and click **Done**.

From now on, sign-in asks for a code from the app. If you lose your phone, use **Use a recovery code instead**: each code works once. You can regenerate a fresh set on your profile.



For administrators

To make 2FA mandatory for everyone, tick **Require 2FA setup** in System → Settings. Users without 2FA are then asked to set it up at their next sign-in.

25 Set up a new product line

Before the first product can be tagged, Hashentic needs to know what the product line looks like. We will set up the Heritage Chronograph watch from the examples.

1. Prepare shared lists (optional)

- 1 Open **Catalog** → **Lookups** and click **Create lookup**. Name it, for example, *Case materials*.
- 2 Open the lookup and click **Create item**. Add items one by one, or switch to **Multiple mode** and upload a CSV or Excel file with value, label and description columns (Multiple mode needs the Bulk write license feature and the Write products permission).

2. Create the asset

- 1 Open **Catalog** → **Assets** and click **Create asset**.
- 2 Enter the **Name** and a **Description**. If the line has a fixed run, enter the **Amount** and tick **Limited**. If you already have a preset for this kind of product, choose it in **Use preset**.
- 3 Tick **GS1 compliant** to use GTINs and GS1 Digital Link, or **DPP compliant** for a Digital Product Passport, and complete the extra steps.
- 4 Click **Create**. The asset page opens.

3. Define the fields

- 1 Open the **Fields** tab and add a field for each piece of data, such as *Serial number* (Text, Required, Show in grid), *Case material* (Lookup) or *Production date* (Date, only past dates).

- 2 Choose the **Field stage**: **Create** for data known at production, **Update** for data added later, such as *Sold at*.
- 3 Tick **Protected** for personal data and **Hidden** for anything customers should not see.

Asset field — Case material

Attributes

Display name *

Case material

Property name

caseMaterial

Type

Lookup

Lookup

Case materials

Options

☒ Required
 ☐ Protected
 ☐ Hidden
 ☐ Show in grid

Field stage

☒ Create
 ☐ Update

Data audience (DPP)

☒ Public
 ☐ Authority
 ☐ Recycler
 ☐ Repairer

Submit

Cancel

A Lookup field drawing its values from the *Case materials* list.

4. Set the protection rules

- 1 On the **Settings** tab, add the countries where the line is sold to **Authorized regions**, so gray-market scans raise alerts.
- 2 Optionally switch on **Answer customer questions with AI** and write a welcome text.
- 3 Add **Labels** you will use later, such as *Boutique stock* and *Sold*.

✓ Reuse it

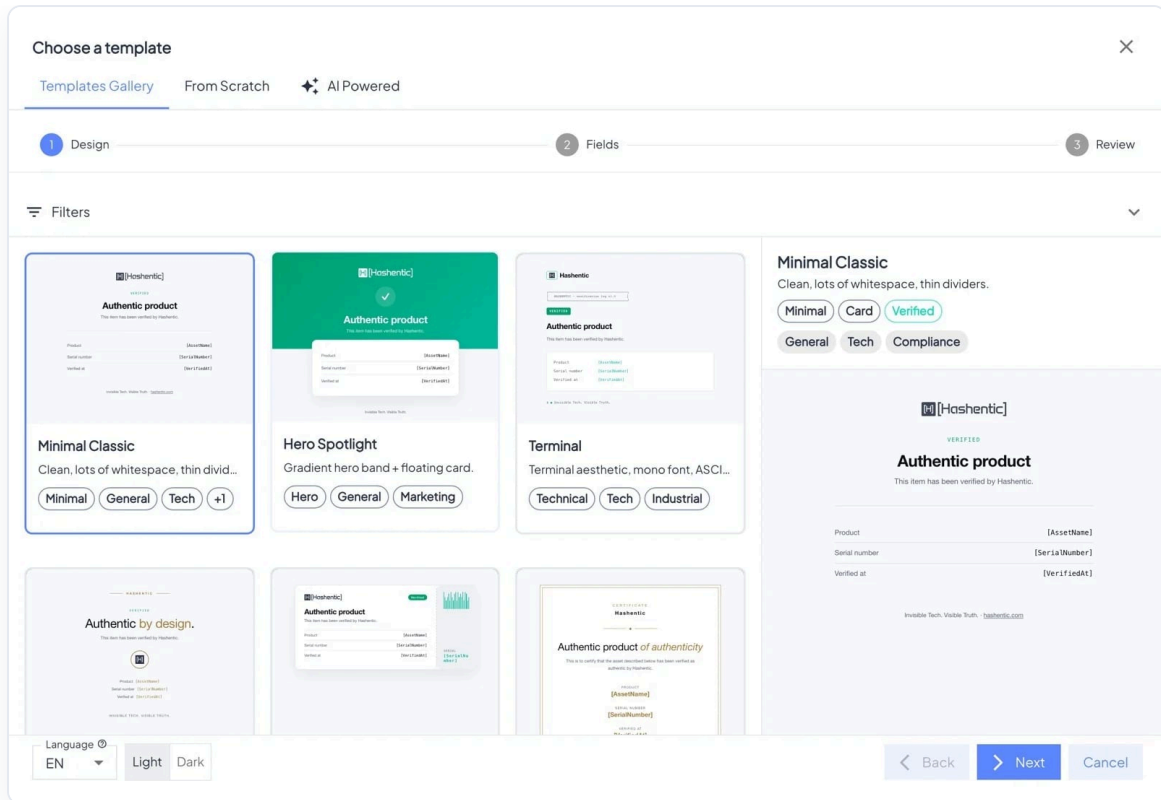
Happy with the structure? Recreate it as a preset in **Catalog** → **Presets** and pick it the next time you create a similar asset.

GUIDE · MARKETING

26 Design the verification page

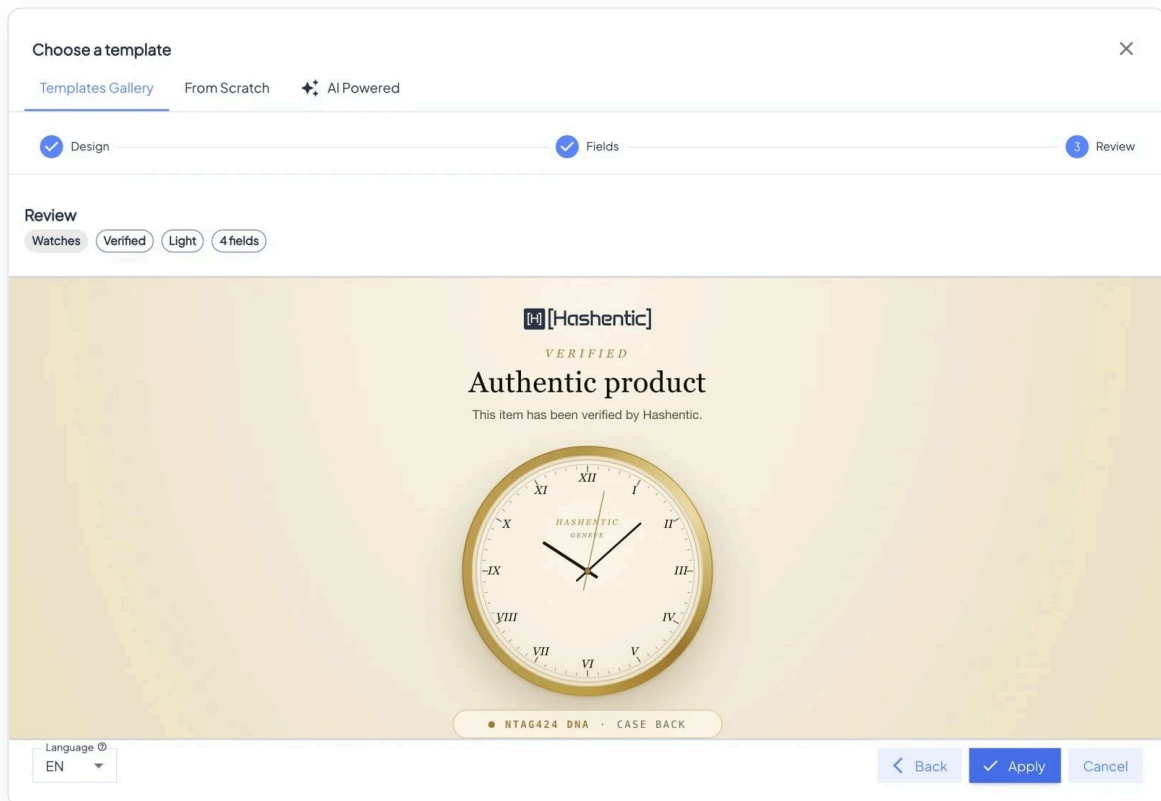
Pick a design from the gallery, choose what it shows, and preview it before customers see it.

- 1 Open the asset and go to the **Templates** tab. Under **Verified page template** click **Choose a template**.



The gallery. Open **Filters** to search, or filter by style, use case and layout.

- 2 Click a design to preview it. Switch between **Light** and **Dark** and the page language, then click **Next**.
- 3 On the **Fields** step, tick the fields to show and order them with the arrows. **Smart defaults** picks a sensible set. Click **Next**.
- 4 On **Review**, check the result and click **Apply**.



Review step: the watch page with the chosen fields.

- Optional: set the **Button color** for the documents and assistant buttons, or click **Edit Template** to adjust texts and images in the block builder.
- For failed scans, keep **Use global template** (designed in System → Settings) or design a page just for this asset.
- Check the result on any product: open it and click **Preview**.

i Different pages for different scans

On the **Auth templates** tab, **New template** adds a page that applies only to certain tag types, labels or countries, for example a notice for scans outside your markets, or a staff page for products labelled *Boutique stock*.

GUIDE · MARKETING

27 Translate the verification page

Show the product page in your customers' languages. AI drafts the translation; you check it and save.

- Open the asset and go to the **Templates** tab. Save the verified page template first if you changed it.
- In the **Languages** bar under the template, click **Add language**.
- The first time, set the **Language of the base content**: the language the template is written in now.
- Choose the **New language** from the list, or type a code such as **pt-BR**.
- Pick **Translate with AI**, or **Copy the base content and translate it myself**, and click **Add**.

Add a language [X]

Language of the base content
English (en)

The language the current template is written in
New language
German (de)

Pick from the list or type a code such as pt-BR

☐ Copy the base content and translate it myself

☒ Translate with AI

[Add] [Cancel]

Adding German to a template written in English.

- Open the new language and click **Edit** to check product names, claims and legal texts. Save.
- Do the same for the unverified page and for every auth template and failed page rule your customers may see.
- Test it: set your phone or browser to that language and scan a product.

✓ When the base page changes

Languages are separate copies. After you change the base template, open each language and click **Translate again with AI** (this replaces your edits to that language), or edit it by hand.

28 Show a different page when a scan fails

Tell customers in plain words what happened: a reused link, a withdrawn product and a suspected copy each get their own page.

- 1 Open the asset, go to the **Auth templates** tab and scroll to **Failed page rules**. Click **New rule**.
- 2 Name it, for example *Link already used*. Under **Failure reasons** choose **Already scanned**.

The rule for links that were already used.

- 3 Under **Page template**, design the page: for example "This link was already used. Tap the tag again to check the product." Save.
- 4 Add a rule *Withdrawn product* for **Blocked or withdrawn**, with your service contact on the page.
- 5 Add a rule for **Authentication failed** with a warning and a way to report a suspected copy. Limit it with **Countries** if the contact differs by market.
- 6 Drag the rules into order. The first rule that matches a failed scan wins; scans that match none show the asset's unverified page.
- 7 Add languages to each rule's page if your customers need them ([Translate the verification page](#)).
- 8 For every product line at once, add the same rules in System → Settings, under the global unverified page template.

i Repeat scans of secure tags

With **Allow already verified asset page** turned on, repeat scans keep showing the product page with a notice, so the *Already scanned* rule is not used. In custom HTML you can also read the failure group from the **[FailReason]** placeholder ([Appendix B](#)).

29 Create QR-coded products and print labels

Create a batch of products from a spreadsheet and print a sheet of QR codes, with no special hardware.

License Bulk write for steps 2–7

- 1 Prepare a CSV or Excel file with one row per product. Name the columns like the asset's fields (the property names, such as **batchNumber**) and they will be matched automatically.

- 2 Open **Catalog** → **Products** → **Add new**, choose **Barcode** and the **Multiple mode** tab.
- 3 Pick the asset in **Asset name**, choose **Upload file** and select your file. (No data per product? Choose **Generate by number** and enter a count.)
- 4 Click **Next**. Check that every field is mapped to the right column in **Set up fields**, then **Next** again.
- 5 Fix any highlighted rows with the edit icon, then click **Generate**. The codes are created in the background; you can close the dialog.
- 6 Open **Operations** → **Bulk operations**. When the run shows *Completed*, click **Download barcodes**.
- 7 In **Export**, choose **PDF**, **QRCode** and the **Public** URL version, pick a size (Medium suits most labels), and on **Caption settings** print a field such as the batch number under each code. Check the grid on **Fixed settings** and click **Generate PDF**.

Caption settings: a field value or your own text under every code.

✓ Single products

For one product, use **Single mode** instead: fill in the values, click **Write**, then **Download** on the product page. **Clone count** prints several copies of the same code.

30 Write NFC tags with the Desktop utility

Secure NFC tags are written at your production or packing station with a USB reader. You need the Desktop utility, a USB NFC reader and blank tags.

Once: install and connect

- 1 In the menu click **Setup desktop utility**, check that **Your platform** is right, and click **Download for ...**. Run the installer.
- 2 Back in the dialog, click **Register desktop utility**. The utility opens and signs in as you. (Or copy the **Desktop application token** from System → Applications and paste it into the utility.)
- 3 When the utility is signed in, the header button turns green: **Connected**. Then plug in the reader; the Add product dialog tells you if the reader is missing.

Write one tag

- 1 Open **Products** → **Add new**, keep **NFC Tag** and **Single mode**, and pick the asset.
- 2 Place a tag on the reader. The admin panel shows the type of the tag on the reader.
- 3 Fill in the product's values and click **Write**. Wait for "Tag written."; the new product's page opens.

Write a batch

- 1 Switch to **Multiple mode**, pick the asset and upload your file (or fetch the records from your ERP). Keep **Save import** ticked.
- 2 Map the fields, fix highlighted rows, and click **Generate**.
- 3 Place the first tag, wait until it is written, remove it, place the next. Progress and any errors are shown per row; use **Retry failed** at the end.
- 4 Interrupted? Open the same asset in Multiple mode again and click **Proceed** to continue where you stopped.

! If the button says "Connect application"

The utility is not running or not signed in with your account. Click the button to start it. If it still does not connect, open the utility's window from the system tray, or register it again from the setup dialog. Once it connects, you can download its logs for support from the header button's menu (**Download logs**).

31 Investigate a fraud alert

A Critical alert has appeared: the same watch was scanned in Paris and, two hours later, in Istanbul, with an older tag counter. Here is how to work it.

- 1 Open **Analytics** → **Fraud alerts**. Use **Add filter** → **Status** = New and **Severity** = Critical to focus.
- 2 Click the alert. Read the **Signals** (here *Cloned chip* and *Impossible travel*), the **Metrics** (distance, speed, counters) and the **Triggering scans**.
- 3 Click **Acknowledge** so colleagues know you are on it.

- 4 Open **Verifications**, search for the product's identifier, and open the clock icon for the full **Verification history** of the tag: where and on which devices it was scanned.
- 5 If the evidence holds, open the product, go to **Authentications**, and choose **Block authentication** for the cloned tag. Every later scan of it fails. (Blocking the whole product from its page needs a tap of the genuine tag, unless the asset allows unprotected management.)
- 6 Back on the alert, click **Confirm fraud**. If it was a false alarm, for example a customer travelling with a VPN, click **Dismiss**.



Look wider

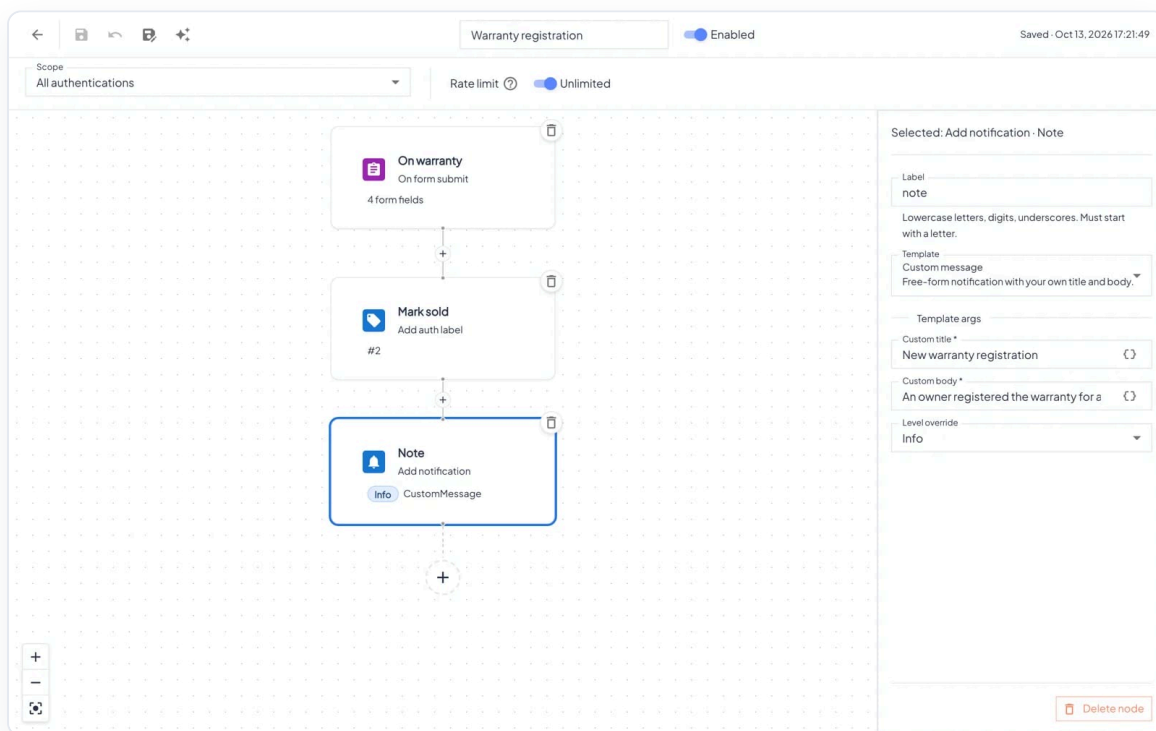
On the **Geo map**, switch on **Invalid** and **Risky** to see whether failed scans cluster in the same place. On the asset, **AI analysis** can summarize what changed: "Are there fraud risks I should look at?"

GUIDE · AUTOMATION

32 Block cloned tags automatically

Let Hashentic act on its own when the fraud engine is sure: block the tag and alert the team, at any time of day.

- 1 Open the asset, go to the **Workflows** tab and click **New workflow**. Name it *Counterfeit response*.
- 2 Click **Add a trigger** and choose **On fraud detected**. In its properties set **Minimum severity** to *High*.
- 3 Click **Add step** → **Add notification**. Choose the *Custom message* template, write a title and text, and set **Level override** to *Critical*.
- 4 Add another step: **Block authentication**.
- 5 Make sure **Enabled** is on and click **Save**.



Editing a step: the properties panel on the right.

Every time a High or Critical alert is raised for this asset, the workflow runs. **Block authentication** acts only on alerts about one specific tag (cloned chip, impossible travel, velocity); for gray-market and invalid-burst alerts it is skipped, but the notification is still sent. Open the runs count in the list to see each run, the product it acted on and the result of every step.

i Prefer a ready-made recipe?

From template... → *Anti-counterfeit: block on second scan* blocks a product the second time it is scanned and notifies you: a good fit for single-use items such as sealed packaging.

GUIDE · CUSTOMER CARE

33 Collect warranty registrations

Turn the moment of verification into a registered customer: a short form after the scan, and the product marked as sold.

- 1 Open the asset's **Forms** tab and click **New form**.
- 2 In the form designer, add a heading and a line of text, then the fields: *Full name* (Text), *Email*, *Purchased at* (Lookup of your boutiques), *Purchase date* (Date). In the settings panel, under **GDPR consent**, turn on the consent checkbox and fill in its text and version.
- 3 Name the form, set **Show this form to** = *All authentications*, tick **Allow only one submission per authentication** and **Allow the customer to skip this form**, and save.
- 4 Go to **Workflows** → **New workflow**. Trigger: **On form submit**, choose your form. Add **Add auth label** → *Sold*, and **Add notification** for your customer-care team. Save.
- 5 Scan a product: the form appears on the verification page. Submissions are listed on the form's row; **Download submissions (CSV)** exports them.

✓ **Privacy**

Mark personal fields such as the email as **Protected** on the asset if you also store them on the product, and set your privacy policy and terms URLs in Branding so the consent checkbox links to them.

GUIDE · ADMINISTRATORS

34 Add a team member

Example: Lucas runs the packing station. He needs to create and tag products, but not change settings or see customer questions.

- 1 Open **System** → **Users** and click **Create user**.
- 2 Enter a **Username** (for example *lucas.meyer*), his **Email** and a starting **Password** (12+ characters, a letter and a digit).
- 3 Choose the **Role** *User* and leave the status *Active*.
- 4 Tick the permissions he needs: Read assets and lookups; Read, Write and Update products; Read and Write bulk operations; Read verifications.
- 5 In **Allowed assets**, select the product lines he works on, and click **Create**.

- 6 Give Lucas his username and starting password through a secure channel, and ask him to set up two-factor authentication.

i Who sees what

Admins see all assets; Users only their allowed assets. The Audit log is reserved for the Super User. To remove access, set the account to *Inactive* (data is kept) or delete it.

GUIDE · OPERATIONS

35 Update many products at once

Example: 40 card holders were moved to the pop-up store and their *Retail status* must change. Fields need the *Update* stage to be editable.

- 1 Open **Catalog** → **Products** → **Update** and switch to **Multiple mode**.
- 2 Collect the products:
 - **Scan**: scan each product's QR code with the webcam or tap tags on the reader; or click **Import from queue** to take the products a colleague scanned with the mobile app.
 - **Query**: pick the asset and filter the products (by label, date, type...). Only assets with *Allow unprotected management* are offered.
- 3 Click **Continue to values**. Under **Shared values**, set the new value for everyone; override individual rows if needed. Click **Continue to review**.
- 4 Check the list and click **Start update**. The update runs in the background and appears in **Bulk operations**, where you can retry anything that failed.

GUIDE · CUSTOMER CARE

36 Help the AI answer your customers

The assistant on the verification page can only be as good as the information you give it. Use what customers ask to fill the gaps.

- 1 Turn the feature on: **System** → **Settings** → tick **Answer customer questions on the verification page**, then on each asset's **Settings** tab tick **Answer customer questions with AI** and write a welcome text.
- 2 After a week, open **Analytics** → **Customer questions** and click the **No information** tile. These are the questions your data could not answer.
- 3 Group the gaps: care instructions, warranty terms, ingredients, servicing.
- 4 Upload the answer: on the asset's **Documents** tab (or **Settings** → **Brand documents** for brand-wide topics) click **Upload** and add a PDF, DOCX, TXT or Markdown file.
- 5 On the document's row choose **Edit**, set **Audience** to *Public* and the language, and save. Wait until the status chip shows *Indexed*.
- 6 Check **Thumbs down** regularly: these answers were not helpful to the customer.



What the assistant will not do

It answers only from public product data and public documents, in the language of the question. It refuses to confirm authenticity (the scan does that), to discuss unrelated topics, or to handle personal data.

GUIDE · FIELD STAFF

37 Connect the mobile app

Sign in on your phone in seconds by scanning a code from the admin panel; no typing of server addresses or passwords.

- 1 Install the Hashentic app on your phone. On Android, the admin panel offers the download: menu → **Mobile app** → **Download APK**, or scan the code shown there.
- 2 In the admin panel open **System** → **Applications** and, under **Sign in on mobile**, click **Show QR code**.
- 3 On the phone tap **Staff sign-in** → **Sign in by scanning QR**, allow the camera and scan the code. The code is valid for up to two minutes (a new one appears automatically) and works only once.
- 4 If your account uses two-factor authentication, enter the code on the phone. The web page confirms: "Successfully signed in on your phone."
- 5 Recommended: protect the app with a PIN or Face ID under **App lock**.

You can now scan products, look them up, edit their data and write NFC tags from the phone. To open a specific product, scan the **QR for the mobile app** on its page in the admin panel.



Reference

Lists to look things up in: why scans fail, what you can put into a page template, languages and limits, and answers to common questions.

A Verification failure reasons

B Template placeholders

C Languages, formats and limits

D Troubleshooting and FAQ

A Verification failure reasons

The Reason shown on the Invalid tab of Verifications, and what it usually means.

Reason	When it happens	Usually means
Invalid product	The code or link is unknown, its product was deleted, or an NFC tag was not finished writing.	Fake or mistyped code
Invalid PICC	NTAG 424: the encrypted tag data does not decrypt to the expected tag.	Forged or cloned tag
Invalid CMAC	NTAG 424: the tag's cryptographic signature is wrong.	Tampered or copied link
Invalid signature	EM4425: the signed data is malformed or the signature is wrong.	Forged tag
Invalid UID	The tag's unique ID does not match the one registered for the product.	Swapped or forged tag
Invalid transaction	The link's transaction does not match the product's integrity record.	Manipulated link
Already verified	A secure tag's one-time code was used before: the same link was opened again.	Re-shared link or replay
Read counter mismatch	The tag's counter went backwards compared with earlier scans.	Cloned tag
Product is blocked	The product was blocked by your team or a workflow.	Stolen, recalled or suspect item
This authentication has been blocked	This particular tag or code was blocked.	Known copy of a tag
This product is only available for internal verification	The product line is restricted to internal checks.	Not for public scanning
Unspecified	An unexpected error during the check.	Contact support if frequent

Reasons in failed page rules

[Failed page rules](#) group the reasons, so one rule covers related failures:

Rule condition	Reasons
Already scanned	Already verified
Blocked or withdrawn	Product is blocked · This authentication has been blocked
Internal use only	This product is only available for internal verification
Authentication failed	Every other reason in the table above

Barcodes and NTAG 215

These carry a fixed link and cannot detect copies on their own: every scan of a copied QR code is valid. Watch them with the *Velocity spike* and *Gray market* fraud signals, and block codes that are clearly being copied.

APPENDIX

B Template placeholders

In block-builder and custom HTML templates, words in square brackets are replaced with real values when the page is shown. Names are not case-sensitive; unknown placeholders stay as they are.

Placeholder	Replaced with
[AssetName]	The asset's name
[AssetDescription]	The asset's description
[VerifiedAt]	Date and time of the verification (UTC)
[VerifiedDate]	Date of the verification
[VerificationMethod]	The carrier type that was scanned
[propertyName]	The product's value for any asset field, e.g. [serialNumber], [caseMaterial]
GS1 fields	For GS1 assets: [gtin], [brandName], [tradeItemDescription], [netContent], [batchLotNumber], [expiryDate] and the other GS1 attributes
Passport data	Any top-level item of the asset's product passport, by its key
[TransactionId] · [TransactionLink]	The integrity record and its explorer link, when assets are stored on a blockchain
[ErrorMessage]	On the unverified page only: why the check failed
[FailReason]	On the unverified page only: the failure group as a code, <code>already-scanned</code> , <code>blocked</code> , <code>internal-only</code> or <code>auth-failed</code> , for example to switch texts in custom HTML

! Hidden fields

A placeholder fills in the value even if the field is marked *Hidden*. Only put fields on a page that customers may see.

The [Integration guide](#) in the admin panel (*Custom HTML templates*) explains how custom HTML pages can also read the full verification data with a script, and how an external website receives it.

APPENDIX

C Languages, formats and limits

Item	Value
Admin panel languages	English, Deutsch, Español, Polski, Русский, 中文
Verification page assistant, documents and forms	Same six languages, following the visitor's browser; AI answers follow the language of the question

Item	Value
Page template languages	Base content plus up to 10 languages per template; the visitor's browser language decides
Built-in verification page	The six admin panel languages, following the visitor's browser
Mobile app languages	English and Russian, following the phone
NFC tags	NTAG 424 DNA, NTAG 215, EM4425
Barcodes	QR code, DataMatrix, Code 128; GS1 Digital Link and GS1 element strings for GS1 assets
Field types	Text, Email, Number, Select, Lookup, Date, Checkbox
Import files	CSV (comma, semicolon, tab or pipe), XLSX, XLS; up to 100,000 rows and 10 MB
Generate by number	Up to 50,000 products at once
Barcode bulk operations	Up to 200,000 records; bulk updates up to 50,000 items
ERP fetch	Preview 50 records; fetch up to 100,000
Documents	PDF, DOCX, TXT, Markdown; 10 MB each by default (up to 25); up to 20 per product, 50 per asset, 100 brand-wide
Labels	Up to 15 per asset
Passwords	12–128 characters with at least one letter and one digit; 5 failed sign-ins lock the account for 5 minutes
Recovery codes	10 single-use codes per user
Desktop utility	Windows x64; macOS Apple Silicon and Intel; USB NFC readers
Mobile app	Android 8.0+; iPhone with iOS 16.4+; NFC-capable phone for tags

Your license adds its own limits: users, assets, tags, barcodes, products, AI usage, document storage, workflow runs and customer questions. See [System → License](#) for your current usage.

APPENDIX

D Troubleshooting and FAQ

A menu item from this guide is missing.

It needs a permission you do not have, or a feature your license does not include. Ask your administrator which permissions and license features your account has.

"Write" stays disabled in Add new.

Hover over it to see why: no asset selected, the Desktop utility or reader is not connected, no tag on the reader, the tag type is not in your license, or a tag or barcode limit has been reached. Empty required fields are reported when you click Write.

The header button says "Connect application" although the utility is running.

The utility is signed in with another account, or from another computer. Register it again from Setup desktop utility, or regenerate the Desktop application token and paste it in.

A customer says a genuine product shows "not verified".

Look the product up in Verifications → Invalid. "Already verified" means they reopened an old tag link: they should tap the tag again, or you can turn on *Allow already verified asset page*. "Product is blocked" means someone blocked it.

A customer sees the verification page in the wrong language.

The page follows the language of the visitor's browser. If the template has no version in that language, the base content is shown: add the language on the template ([Translate the verification page](#)).

The dashboard looks empty.

Check the asset picker and the period (D, W, M, Y, All). New scans can take about a minute to appear in charts.

Why are some scans without a country?

Location comes from the scanner's internet address and needs the Geolocation analytics license feature. Scans from private networks cannot be located.

Can I change a field after products exist?

You can edit and add fields, but not delete them or change their property name. Values of existing products can be changed only for fields with the Update stage.

A document is stuck at "Waiting for indexing" or shows "Indexing failed".

Indexing runs in the background and can take a few minutes. Scanned PDFs without a text layer cannot be read: upload a text-based PDF and use Re-index.

Workflows with an HTTP request cannot be saved.

Add the address pattern (for example `https://crm.example.com/*`) to Settings → Workflows URL allowlist first.

How do I give an auditor read-only access?

Create a User with only read permissions (products, verifications, assets) and the relevant allowed assets. Changes are recorded in the Audit log.

Where can developers learn about the API and webhooks?

Open **Integration guide** at the bottom of the menu: guides for custom HTML templates, workflows, the REST API, webhooks and ERP integration.