[Hashentic]

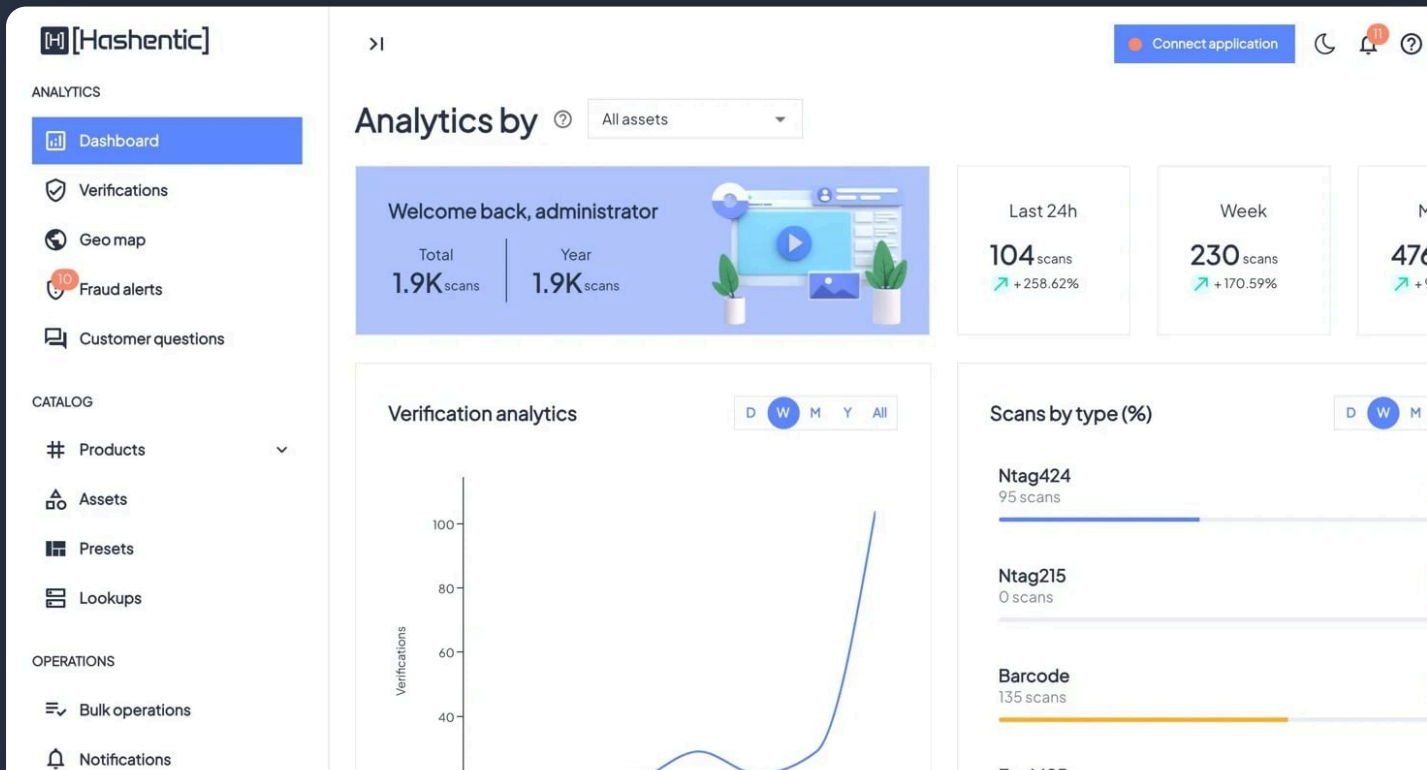
Funktionen und Benutzerhandbuch
Ausgabe Oktober 2026

PLATTFORM ZUR PRODUKTAUTHENTIFIZIERUNG

Funktionen und Benutzerhandbuch

Was Hashentic für Ihre Marke leistet und wie Sie es einsetzen: vom ersten gekennzeichneten Produkt bis zur Bearbeitung eines Fälschungsalarms.

Administrationsbereich | Verifizierungsseite | Mobile App | Desktop-Dienstprogramm



INHALT

Was Sie hier finden

Teil I Überblick 4

1 Hashentic auf einen Blick 5

2 Grundbegriffe 7

3 Rollen, Berechtigungen und Ihre Lizenz 8

4 Sich im Administrationsbereich zurechtfinden 10

Teil II Funktionskatalog 12

5 Das Dashboard 13

6 Verifizierungen 14

7 Geografische Karte 16

8 Betrugs- und Anomaliealarme 17

9 Kundenfragen 19

10 Produkte 21

11 Assets und Felder 24

12 Vorlagen für Verifizierungsseiten 28

13 Presets und Lookups 32

14 Labels und Formulare 34

15 Automatisierte Workflows 36

16 Tags beschreiben und Barcodes drucken 38

17 Massenoperationen und ERP 41

18 Benachrichtigungen und Audit-Protokoll 43

19 KI-Funktionen 45

20 Benutzer und Zugriff 47

21 Einstellungen, Branding und Lizenz 48

22 Mobile App und Desktop-Dienstprogramm 53

23 Die Verifizierungsseite für Verbraucher 56

Teil III Schrittanleitungen 58

24 Ihr Konto absichern 59

25 Eine neue Produktlinie einrichten 59

26 Die Verifizierungsseite gestalten 61
27 Die Verifizierungsseite übersetzen 62
28 Bei fehlgeschlagenen Scans eine andere Seite anzeigen 63
29 Produkte mit QR-Code anlegen und Etiketten drucken 64
30 NFC-Tags mit dem Desktop-Dienstprogramm beschreiben 66
31 Einen Betrugsalarm untersuchen 67
32 Geklonte Tags automatisch sperren 67
33 Garantieregistrierungen erfassen 68
34 Ein Teammitglied hinzufügen 69
35 Viele Produkte gleichzeitig aktualisieren 69
36 Die KI bei Kundenantworten unterstützen 70
37 Die mobile App verbinden 70
38 Hashentic mit Shopify nutzen 71

Anhang **Nachschlagewerk** **77**

A Gründe fehlgeschlagener Verifizierungen 78
B Platzhalter in Vorlagen 79
C Sprachen, Formate und Limits 80
D Fehlerbehebung und häufige Fragen 81

Überblick

Was Hashentic ist, die Grundbegriffe, auf denen alles aufbaut, und die Orientierung im Administrationsbereich.

01 Hashentic auf einen Blick

02 Grundbegriffe

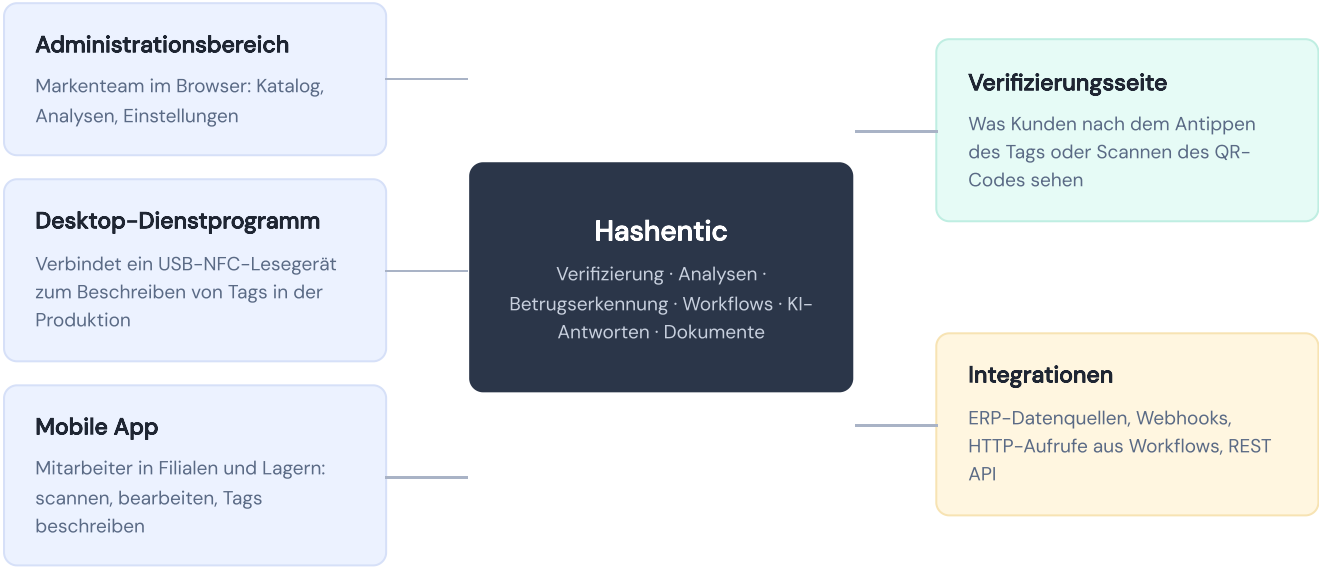
03 Rollen, Berechtigungen und Ihre Lizenz

04 Sich im Administrationsbereich zurechtfinden

ÜBERBLICK

1 Hashentic auf einen Blick

Hashentic gibt jedem physischen Produkt eine digitale Identität, die Kunden durch kurzes Antippen prüfen können. Sie definieren Ihre Produktlinien, kennzeichnen jeden Artikel mit einem sicheren NFC-Tag oder QR-Code und Hashentic prüft jeden Scan, zeigt eine Seite im Markendesign und informiert Sie darüber, wo, wann und wie Ihre Produkte geprüft werden.



So wird ein Produkt geschützt

1 · Beschreiben

Erstellen Sie ein **Asset** für jede Produktlinie mit den gewünschten Feldern (Seriennummer, Material, Charge …) und der Seite für Ihre Kunden.

2 · Kennzeichnen

Erstellen Sie **Produkte** und versehen Sie jedes mit einer Authentifizierung: einem kryptografischen NFC-Tag, beschrieben mit dem Desktop-Dienstprogramm oder der mobilen App, oder einem gedruckten QR-/Barcode-Etikett.

3 · Beobachten

Jeder Scan wird geprüft und erfasst. Dashboards, geografische Karte und Betrugsalarme zeigen echte Nachfrage, Graumarkt-Abflüsse und Kopien.

Ihre Möglichkeiten

- Authentifizieren Sie Produkte mit sicheren NFC-Tags **NTAG 424 DNA** und **EM4425**, **NTAG 215** oder QR-/DataMatrix-/Code-128-Barcodes einschließlich GS1 Digital Link.
- Verfolgen Sie jeden **gültigen und ungültigen Scan** mit Datum, Land, Gerät und Risikohinweisen.
- Beschreiben Sie Tags einzeln oder **gesammelt** aus einer Tabelle oder einem ERP und drucken Sie Barcode-Bögen als PDF.
- Erfassen Sie Garantieregistrierungen und Anmeldungen über **Formulare** auf der Verifizierungsseite.
- Steuern Sie den Zugriff mit **Rollen und detaillierten Berechtigungen**, Zwei-Faktor-Anmeldung und einem vollständigen Audit-Protokoll.
- Gestalten Sie **Verifizierungsseiten** im Markendesign aus über 60 Vorlagen, mit KI-Assistent und Produktdokumenten direkt auf der Seite.
- Erkennen Sie **geklonte Tags, unmögliche Reisen, Graumarktverkäufe** und Scan-Häufungen automatisch.
- Automatisieren Sie Reaktionen mit **Workflows**: Tags sperren, Produkte kennzeichnen, das Team benachrichtigen, Ihre Systeme aufrufen.
- Bereiten Sie Daten für den **Digitalen Produktpass** vor (GS1, Wirtschaftsakteur, Kreislauffähigkeit, EU-Batteriepass).
- Nutzen Sie den Administrationsbereich in **sechs Sprachen**: Englisch, Deutsch, Spanisch, Polnisch, Russisch und Chinesisch.

Zu den Beispielen in diesem Handbuch

Alle Bildschirmaufnahmen stammen aus einem Demo-Arbeitsbereich der fiktiven Marke **Kestrel & Vine**, die Uhren, Lederwaren und einen Duft verkauft. Namen, Zahlen und Scans sind erfunden. Ihre Ansichten zeigen Ihren eigenen Katalog; einige Menüs erscheinen nur, wenn Ihre Lizenz und Berechtigungen sie einschließen.

ÜBERBLICK

2 Grundbegriffe

Einige Begriffe begegnen Ihnen auf fast jeder Seite. Wenn Sie diese kennen, erschließt sich der übrige Administrationsbereich leicht.

Asset

Eine Produktlinie oder ein Modell, etwa "Heritage Chronograph 42". Es definiert die Felder jedes Artikels, das Design der Verifizierungsseite, Betrugsregeln, Formulare und Workflows. Ein Asset kann auf eine feste Produktanzahl begrenzt sein.

Produkt

Ein physischer Artikel eines Assets mit eigenen Werten (Seriennummer, Charge …) und einer kurzen **Kennung** wie **7eWb86L**. Produkte können gesperrt oder gelöscht werden.

Authentifizierung

Der Datenträger, der die Echtheit eines Produkts belegt: ein NFC-Tag (NTAG 424, NTAG 215, EM4425) oder ein Barcode/QR-Code. Ein Produkt kann mehrere besitzen.

Verifizierung

Ein einzelner Scan einer Authentifizierung durch eine beliebige Person. Er ist **gültig** oder **ungültig**, mit einem Grund wie "Invalid CMAC" oder "Product is blocked".

Feld

Eine am Asset definierte Produktangabe: Text, Email, Number, Select, Lookup, Date oder Checkbox. Felder können erforderlich, geschützt (verschlüsselt), vor Verbrauchern verborgen oder später bearbeitbar sein.

Preset

Eine wiederverwendbare Kombination aus Feldern und Seitenvorlage. Wählen Sie beim Anlegen eines Assets ein Preset, um stets mit derselben Struktur zu beginnen.

Lookup

Eine verwaltete Werteliste (Materialien, Boutiquen, Märkte …), aus der Lookup-Felder ihre Werte beziehen, damit alle dieselbe Schreibweise verwenden.

Label

Eine farbige Kennzeichnung an einem Produkt oder einer Authentifizierung, etwa "Verkauft" oder "In Wartung". Labels steuern Vorlagen, Formulare und Workflows.

Vorlage

Die Verifizierungsseite für Kunden. Jedes Asset besitzt eine Seite für gültige Scans, optional eine für ungültige Scans und optionale **Auth-Vorlagen** für bestimmte Länder, Labels oder Tag-Typen.

Workflow und Formular

Workflows reagieren mit Aktionen auf Ereignisse (Scan, Sperre, Betrugsalarm, Formular, Webhook). Formulare erfassen Kundeneingaben auf der Verifizierungsseite.

✓ **Tags und Barcodes in einem Satz**

Sichere NFC-Tags (NTAG 424 DNA, EM4425) erzeugen bei jedem Antippen einen neuen kryptografischen Code; ein kopierter Link wird deshalb erkannt. Barcodes und NTAG 215 enthalten einen festen Link: Sie sind günstiger und druckbar, doch eine Kopie wird als echt gescannt. Überwachen Sie sie mit Betrugsalarmen (Scanrate, Graumarkt).

ÜBERBLICK

3 Rollen, Berechtigungen und Ihre Lizenz

Was eine Person sehen und tun kann, hängt von zwei Dingen ab: den **Berechtigungen** ihres Kontos und den **Funktionen** der Unternehmenslizenz. Fehlt ein hier beschriebener Menüpunkt, ist eines davon der Grund.

Rollen

Rolle	Bedeutung
Superuser	Die höchste Rolle, die das integrierte Konto **administrator** besitzt. Hat sämtliche Berechtigungen, sieht jedes Asset und kann als einzige Rolle das Audit-Protokoll öffnen. Ein Superuser kann diese Rolle anderen Konten zuweisen.
Administrator	Sieht alle Assets und kann genau das tun, was die am Konto aktivierten Berechtigungen erlauben.
Benutzer	Arbeitet innerhalb seiner Berechtigungen nur mit den dem Konto zugewiesenen Assets.
Behörde · Recyclingbetrieb · Reparaturbetrieb	Partnerrollen für den Digitalen Produktpass. Sie lesen, aktualisieren und sperren Produkte zugewiesener DPP-Assets und sehen oder bearbeiten nur Felder, deren Datenzielgruppe ihre Rolle einschließt.

Berechtigungen

Im Benutzerformular sind Berechtigungen nach Bereichen gruppiert: Products, Assets, Presets, Lookups, Workflows, AI, Users, Settings, License, Integrations und Notifications management (siehe Benutzer und Zugriff). Eine Schreibberechtigung erteilt zugleich die zugehörige Leseberechtigung. Die wichtigsten:

Gruppe	Berechtigungen
Products	Produkte lesen, schreiben, aktualisieren, löschen, sperren, entsperren; gültige und ungültige Verifizierungen lesen; Massenoperationen lesen/schreiben; Betrugsalarme lesen/schreiben
Assets, Presets, Lookups	Assets lesen, schreiben, löschen; Presets lesen/schreiben; Lookups lesen/schreiben
Workflows	Workflows lesen/schreiben; Workflow-Vorlagen schreiben; Audit-Ereignisse lesen
AI	KI-Felder, Vorlagen, Empfehlungen und Workflows erzeugen; KI-Analyse nutzen; KI-Assistent nutzen; Kundenfragen lesen
Administration	Benutzer lesen/schreiben; Einstellungen lesen/schreiben; Lizenz schreiben; ERP-Verbindungen verwalten; Benachrichtigungen lesen

Lizenzfunktionen

Ihre Lizenz hat einen Tarif (Free, Start, Pro, Business oder Enterprise; ein neues Konto beginnt mit einer Testphase, Trial, die 30 Tage dauert, sofern nicht anders festgelegt, und wechselt danach zu Free) und aktiviert optionale Funktionen. Der Tarif legt **monatliche** Limits für Scan-Analysen, neue QR-Codes und NFC-Schreibvorgänge fest sowie Gesamtlimits für Benutzer, Produktlinien und Dokumentenspeicher. Über die Monatsmenge hinaus können Sie nur Prepaid-Pakete nutzen, die Ihre Administration auf der Lizenzseite bestellt und per Rechnung bezahlt (siehe Paket bestellen). Scans selbst werden nie blockiert. Einzelheiten finden Sie unter Lizenz. Funktionen mit erforderlicher Lizenzoption sind in diesem Handbuch mit einem **Lizenz** Funktionschip markiert.

Hat Ihr Unternehmen mehr Benutzer oder Produktlinien, als der Tarif erlaubt, etwa nach dem Ende der Testphase oder einem Downgrade, arbeiten die ältesten innerhalb des Limits weiter. Superuser können sich immer anmelden und zählen zuerst; weitere aktive Benutzer über dem Benutzerlimit können sich nicht anmelden, und Produktlinien über dem Produktlinienlimit nehmen keine neuen

Produkte auf. Welche zählen, bestimmen Sie, indem Sie Benutzer deaktivieren oder löschen bzw. Produktlinien löschen, oder Sie wechseln in einen höheren Tarif. Vorhandene Produkte und Codes werden weiter verifiziert. Gelöschte Dokumente zählen zum Dokumentenspeicher, solange sie wiederhergestellt werden können (7 Tage).

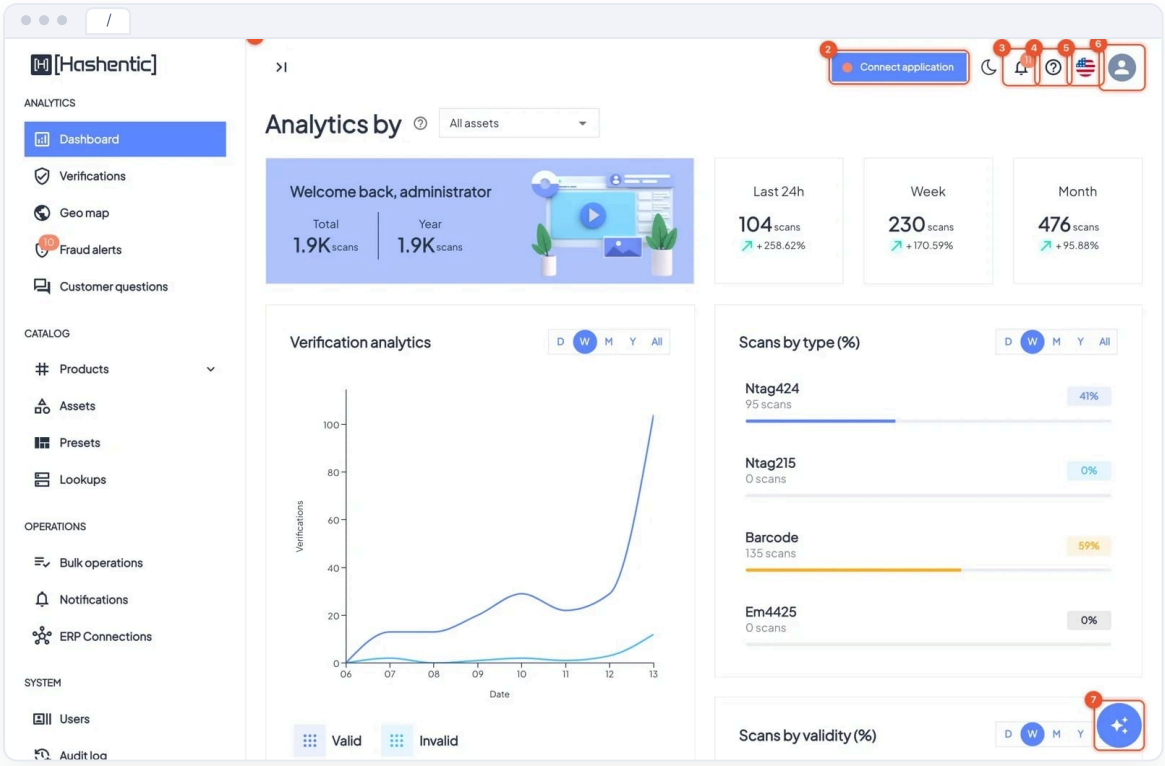
Funktion	Freigeschaltete Möglichkeiten
Bulk write	Multiple mode zum Beschreiben von Tags und Erzeugen von Barcodes, Massenoperationen, ERP-Verbindungen
Update records	Produktwerte nach dem Anlegen bearbeiten
Geolocation analytics	Land jedes Scans, geografische Karte, Länderregeln in Vorlagen und Betrugserkennung
Device info analytics	Gerät, Marke, Modell und Betriebssystem jedes Scans
Fraud detection	Betrugsalarme, Betrugseinstellungen, Workflow-Auslöser "On fraud detected"
Workflows · Asset forms	Workflow-Editor und Durchläufe · Formulare auf der Verifizierungsseite
AI · AI analysis · AI assistant · Customer AI	KI-Generatoren · Fragen zu Ihren Daten · Assistent im Administrationsbereich · KI-Antworten auf der Verifizierungsseite und Seite Customer questions
Product documents	Dokumentenbibliothek und Dokumente auf der Verifizierungsseite
Product lookup	GS1-Daten beim Anlegen eines Assets anhand einer GTIN ausfüllen
White-label branding	Branding-Seite mit eigenem Namen, Logos, Farben und Links
Mobile applications	Mobile App, Anmeldung per QR-Code, Tags per Telefon beschreiben

Ihre Lizenz kann auch die erlaubten Datenträgertypen (NTAG 424, NTAG 215, EM4425, Barcode) beschränken. Die Lizenzseite zeigt Ihren Tarif, Status, Daten, die Limits und die Nutzung dieses Monats sowie Ihre gekauften Pakete; fragen Sie Ihre Administration nach dem Funktionsumfang.

ÜBERBLICK

4 Sich im Administrationsbereich zurechtfinden

Der Administrationsbereich funktioniert in jedem modernen Browser. Das linke Menü ist nach Aufgaben gruppiert; die obere Leiste enthält Werkzeuge für alle Seiten.



Der Administrationsbereich. 1 Menü mit Analytics, Catalog, Operations und System · 2 Lesegerätestatus: verbindet das Desktop-Dienstprogramm für NFC-Tags · 3 Benachrichtigungen · 4 Einführung erneut starten · 5 Sprache · 6 Ihr Profil · 7 KI-Assistent.

Das Menü

- **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.
- Unten: **Integration guide**, **Mobile app**, **Setup desktop utility** und Darstellungseinstellungen.

Überall hilfreich

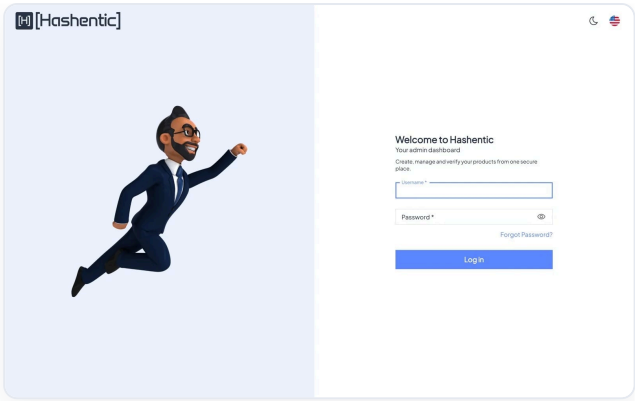
- Das **?** neben einem Seitentitel erklärt die Seite; **Show app tour** startet die Einführung erneut.
- Listen bieten dieselben Werkzeuge: Suchfeld, **Add filter** für genaue Filter, sortierbare Spalten und Seitengröße.
- Wechseln Sie mit dem Mondsymbol zwischen **hell/dunkel** und mit der Flagge die **Sprache**.
- Die **Schaltfläche mit dem Funkensymbol** unten rechts öffnet den KI-Assistenten.

Anmeldung

Öffnen Sie die Hashentic-Adresse Ihres Unternehmens und melden Sie sich mit Benutzername und Passwort an. Je nach Unternehmenseinstellungen erscheint auch **Continue with Google**; möglicherweise wird ein Code aus Ihrer Authenticator-App verlangt (Zwei-Faktor-Authentifizierung).

Passwort vergessen? Klicken Sie auf **Forgot Password?** und folgen Sie dem Link in Ihrer E-Mail. Nach mehreren Fehlversuchen wird das Konto für einige Minuten gesperrt.

Bei Ihrer ersten Anmeldung zeigt eine kurze Einführung die wichtigsten Bereiche. Sie können sie jederzeit erneut starten.



Anmeldeseite. Der Markenname Ihres Unternehmens erscheint im Titel.

II

Funktionskatalog

Jeder Bereich von Hashentic in einem Kapitel: Zweck, Bildschirminhalte und Handlungsmöglichkeiten. Nutzen Sie diesen Teil als Nachschlagewerk; die Schrittanleitungen in Teil III bauen darauf auf.

05 Das Dashboard

06 Verifizierungen

07 Geografische Karte

08 Betrugs- und Anomaliealarme

09 Kundenfragen

10 Produkte

11 Assets und Felder

12 Vorlagen für Verifizierungsseiten

13 Presets und Lookups

14 Labels und Formulare

15 Automatisierte Workflows

16 Tags beschreiben und Barcodes drucken

17 Massenoperationen und ERP

18 Benachrichtigungen und Audit-Protokoll

19 KI-Funktionen

20 Benutzer und Zugriff

21 Einstellungen, Branding und Lizenz

22 Mobile App und Desktop-Dienstprogramm

23 Die Verifizierungsseite für Verbraucher

ANALYSEN

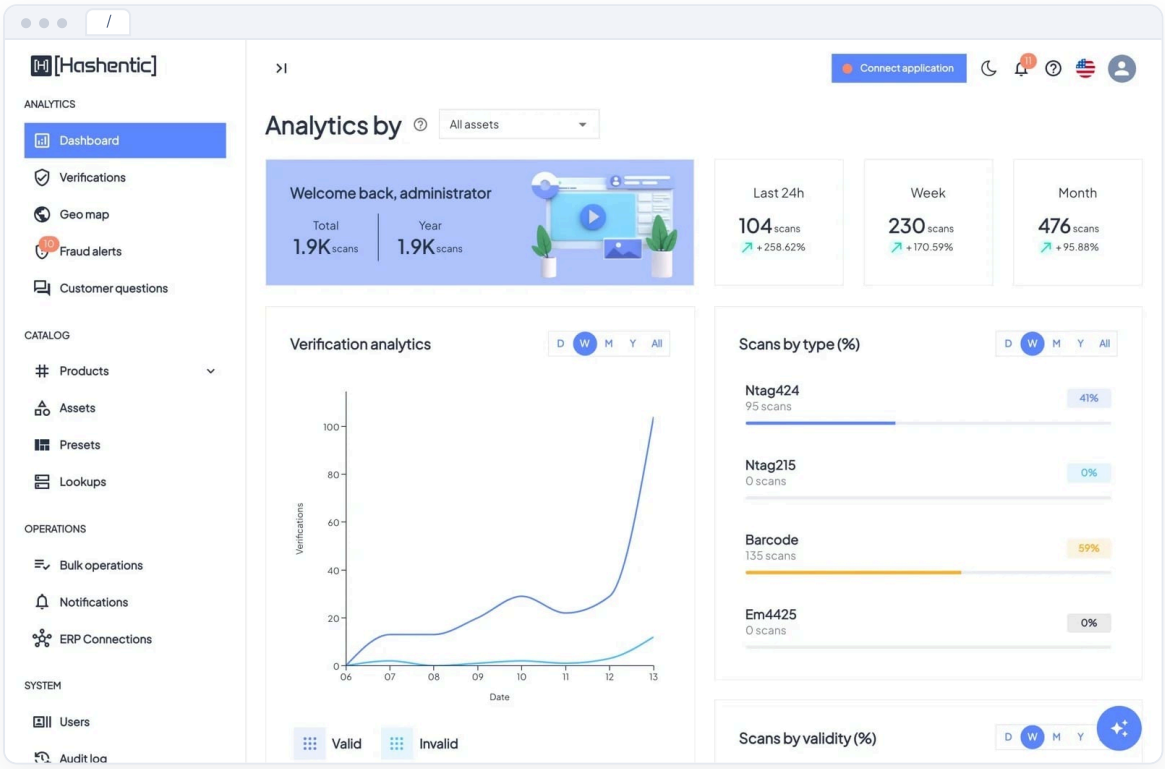
5 Das Dashboard

Die Startseite zeigt die Anzahl echter Scans, ihre Entwicklung, die von Kunden verwendeten Datenträger und deren Standorte.

Menü Analytics → Dashboard

Zugriff alle Benutzer; Daten auf Ihre Assets beschränkt

Lizenz Geolocation analytics für die Länderkarte



Dashboard. Wählen Sie unter **Analytics by** ein Asset aus, um alle Karten auf eine Produktlinie zu beschränken.

- **Willkommenskarte** mit **Total** und **Year** sowie Karten für **Last 24h**, **Week** und **Month** einschließlich Trend gegenüber dem vorherigen Zeitraum. Gezählt werden echte (gültige) Scans.
- **Scans by type (%)**: Anteil der Scans von NTAG 424, NTAG 215, EM4425 und Barcodes.
- **Scans by country**: Weltkarte mit einer Färbung nach Anzahl echter Scans pro Land.
- **Verification analytics**: gültige und ungültige Scans im Zeitverlauf. Wechseln Sie den Zeitraum mit **D** **W** **M** **Y** **All**.
- **Scans by validity (%)**: echte gegenüber fehlgeschlagenen Prüfungen.
- **Details überall öffnen**: Klicken Sie auf eine Zahl, Datenreihe, Typzeile, ein Kreissegment oder ein Land, um die zugehörigen Scans aufzulisten.

Tipp

Die Detailliste zeigt jeden einzelnen Scan mit dem angeklickten Kontext als festem Filter (zum Beispiel "Country: FR"). Klicken Sie auf eine Zeile, um alle Details der Verifizierung zu öffnen.

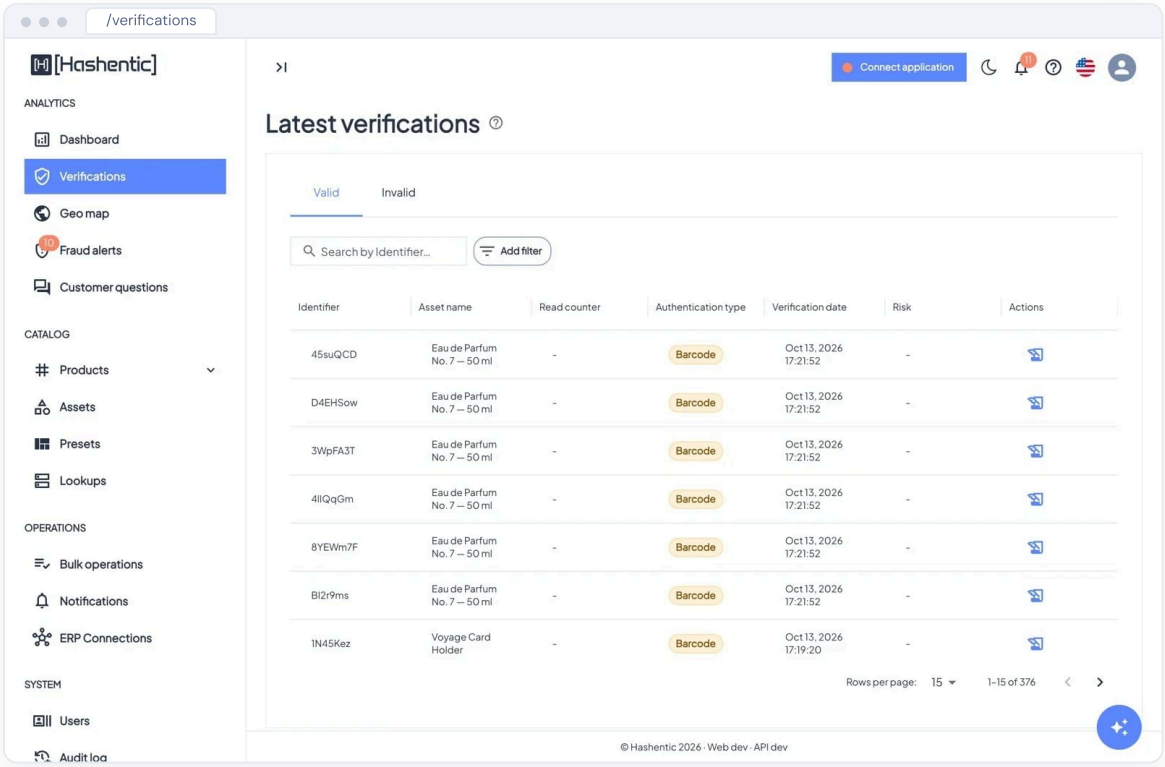
ANALYSEN

6 Verifizierungen

Das Scanprotokoll. Valid zeigt echte Prüfungen, Invalid jeden fehlgeschlagenen Scan mit seinem Grund.

Menü Analytics → Verifications

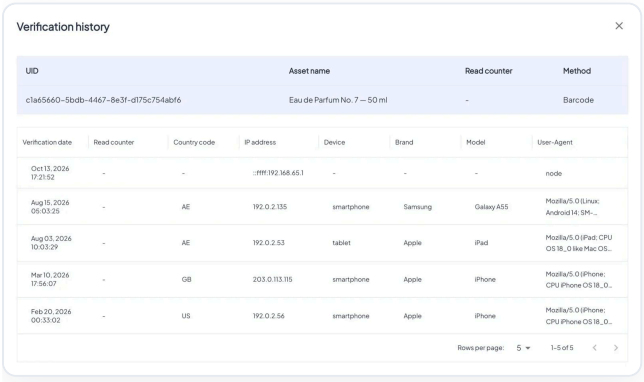
Berechtigung Read valid / invalid product verifications



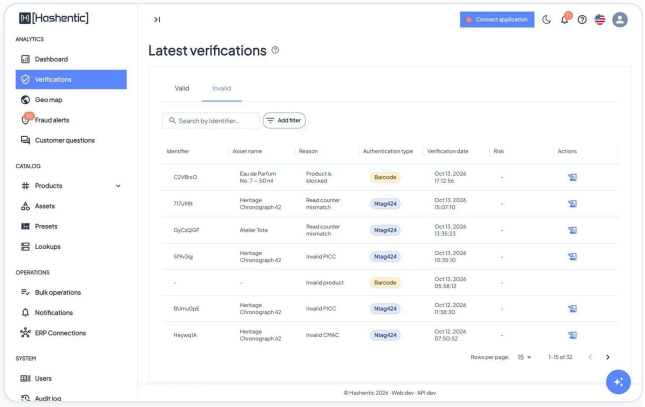
Neueste Verifizierungen. Die Liste zeigt den neuesten passenden Scan jedes Produkts. Das Uhrsymbol öffnet jeden Scan eines Tags; die Dashboard-Detailansicht jeden Scan eines Zeitraums.

Warum schlagen Scans fehl?

Die meisten Fehler entstehen durch Kopien: Ein geklonter NFC-Tag besteht die kryptografische Prüfung nicht ("Invalid CMAC", "Invalid PICC"), ein weitergegebener Tag-Link wird als "Already verified" oder "Read counter mismatch" erkannt und ein erfundener oder gelöschter Code als "Invalid product". Scans gesperrter Produkte schlagen mit "Product is blocked" oder "This authentication has been blocked" fehl.



Verifizierungsverlauf eines QR-Codes: Datum, Land, IP-Adresse und Gerät jedes Scans.



Tab Invalid. Die Spalte Reason erklärt jeden Fehler. Alle Gründe sind in Anhang A aufgeführt.

Spalten

- **Identifier** und **Asset name** des Produkts.
- **Read counter** der NFC-Tags, der mit jedem Antippen steigt ("–" bei Barcodes). Im Tab Invalid steht hier **Reason**.
- **Authentication type**: Ntag424, Ntag215, Em4425 oder Barcode.
- **Risk**: **VPN** , **Proxy** , **Tor** oder **Threat** , wenn der Scan aus einem markierten Netzwerk stammt.

Scans finden

- Suchen Sie nach der Kennung oder nutzen Sie **Add filter** : Identifier, UID, Authentication type, Verification date, Asset name, Country code und im Tab Invalid auch Reason.
- Klicken Sie auf eine Zeile für **Verification info**: Land, IP-Adresse, Gerät, Marke, Modell, Browser und Produktfeldwerte.
- Das Uhrsymbol öffnet die **Verification history** dieses Tags oder Codes: alle Scans in zeitlicher Reihenfolge.

Scans oberhalb des Kontingents **Scan analytics** dieses Monats haben keinen Standort und kein Gerät. IP-Adressen von Scans, die älter als die Aufbewahrungsdauer sind (Standard 365 Tage, siehe Einstellungen), werden gekürzt; Standort, Land und Gerät bleiben erhalten.

ANALYSEN

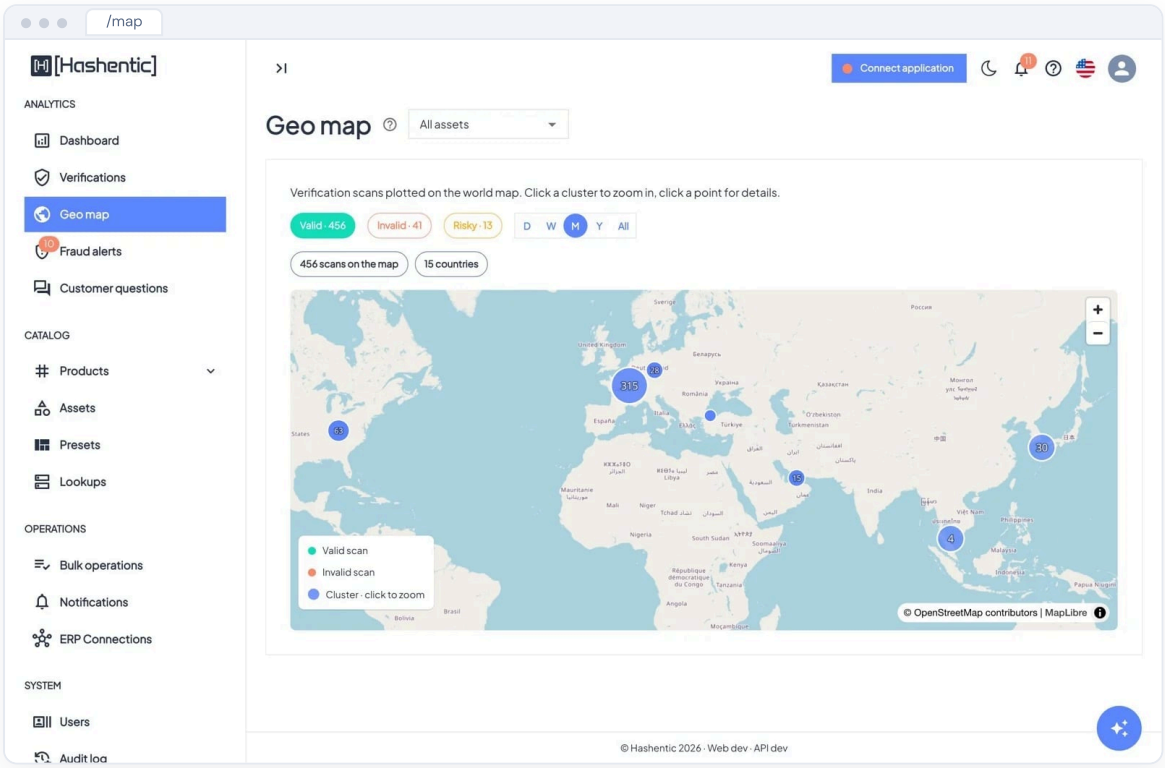
7 Geografische Karte

Alle geografisch zugeordneten Scans auf einer interaktiven Weltkarte zeigen Ihnen, wo Ihre Produkte geprüft werden und wo Kopien auftauchen.

Menü Analytics → Geo map

Berechtigung Read verifications

Lizenz Geolocation analytics



Geografische Karte. Benachbarte Scans werden zu Clustern zusammengefasst. Klicken Sie auf einen Cluster zum Vergrößern und auf einen Punkt für die Scanliste.

- ✓ Blenden Sie Scans mit **Valid**, **Invalid** und **Risky** ein oder aus. Ungültige und riskante Scans (VPN, Proxy, Tor, Bedrohung) sind zunächst ausgeblendet.
- ✓ Die Chips über der Karte zählen die angezeigten Scans und ihre Herkunftsländer.
- ✓ Wählen Sie den Zeitraum (standardmäßig **M**, der letzte Monat) und grenzen Sie die Ansicht auf ein Asset ein.
- ✓ Klicken Sie auf einen Punkt und dann auf **Click to see the list**, um die zugehörigen Scans zu öffnen.

Scans oberhalb des Kontingents **Scan analytics** dieses Monats haben keinen Standort und kein Gerät und erscheinen daher nicht auf der Karte. IP-Adressen von Scans, die älter als die Aufbewahrungsdauer sind (Standard 365 Tage), werden gekürzt; Standort, Land und Gerät bleiben erhalten, die Karte bleibt also unverändert.

ANALYSEN

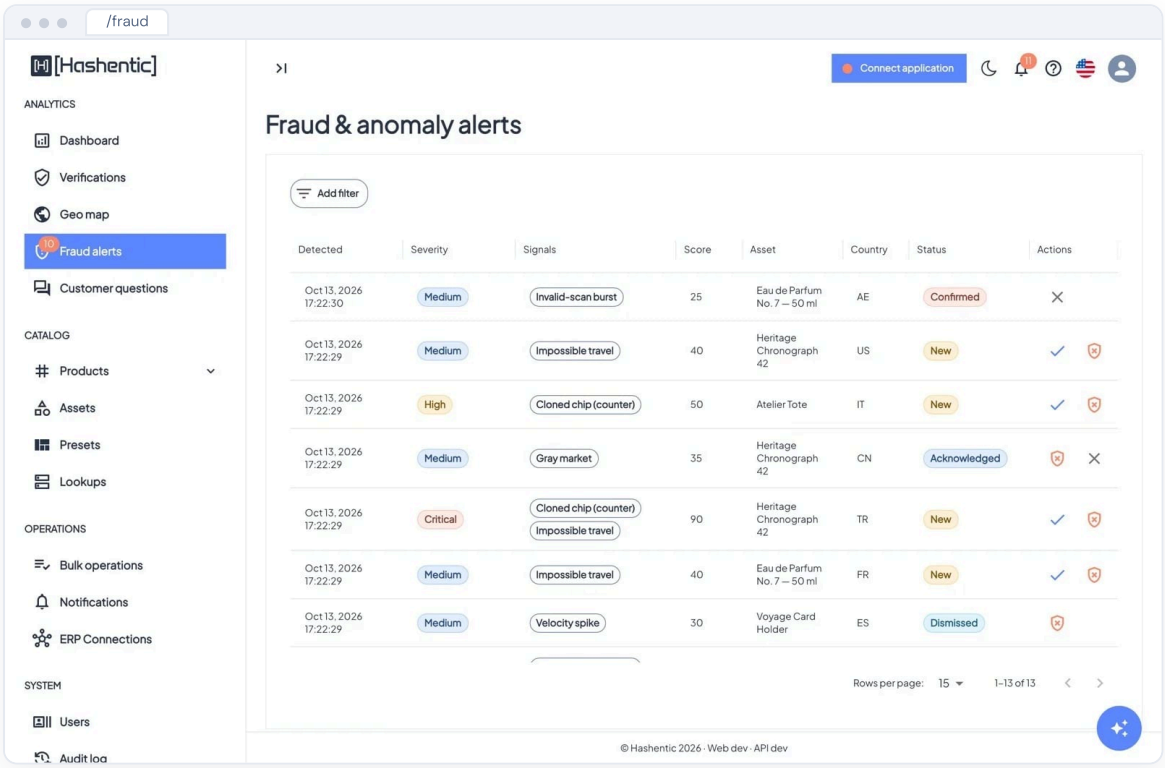
8 Betrugs- und Anomaliealarme

Hashentic überwacht den Scanstrom und löst einen Alarm aus, wenn ein Muster auf Fälschungen oder Vertriebsumleitung hindeutet. Die Menümarkierung zählt Alarme mit dem Status **New**.

Menü Analytics → Fraud alerts

Berechtigung Read fraud alerts (Aktionen: Write fraud alerts)

Lizenz Fraud detection



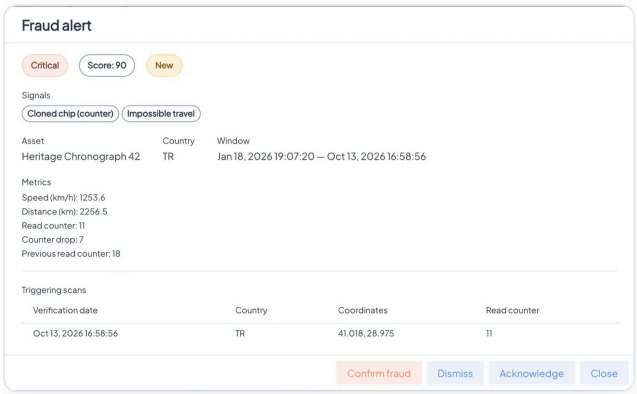
Betrugs- und Anomaliealarme. Jeder Alarm kombiniert ein oder mehrere Signale zu einem Wert und einem Schweregrad.

Was einen Alarm auslöst

Signal	Auslösung, wenn …	Gewicht
Cloned chip (counter)	Ein sicherer NFC-Tag einen Lesezähler meldet, der nicht höher ist als ein bereits bekannter: Zwei physische Tags teilen dieselbe Identität.	50
Impossible travel	Zwei aufeinanderfolgende Scans desselben Tags mehr als 100 km auseinanderliegen und eine Reisegeschwindigkeit über 900 km/h erfordern würden.	40
Gray market	Mindestens 3 echte Scans eines Assets innerhalb von 24 Stunden aus einem Land außerhalb seiner **Authorized regions** stammen.	35
Velocity spike	Derselbe Tag oder Code innerhalb von 10 Minuten mindestens 10-mal gescannt wird.	30
Invalid-scan burst	Ein Produkt innerhalb von 30 Minuten mindestens 5 fehlgeschlagene Scans verzeichnet.	25
Risky IP	Ergänzt ein anderes Signal, wenn ein auslösender Scan aus einem VPN-, Proxy-, Tor- oder Bedrohungsnetzwerk stammt.	15

Der Wert ist die Summe der Gewichte (höchstens 100). Ab 75 ist ein Alarm **Critical**, ab 45 **High**, ab 25 **Medium**. Die High- und Critical-Grenzen sowie Werte für Reise, Scanrate, Graumarkt und Häufungszeitraum lassen sich unter Settings → Fraud & anomaly detection anpassen; die Häufungsanzahl verwendet *Invalid verification anomaly threshold* unter Verification alerts. High- und Critical-Alarme

senden außerdem eine Benachrichtigung und können einen Workflow starten ("On fraud detected").



Alarmdetails. Kennzahlen (Entfernung, Geschwindigkeit, Zählerstände) und auslösende Scans.

Einen Alarm bearbeiten

- **Acknowledge**: Sie haben ihn gesehen und untersuchen ihn.
- **Confirm fraud**: Es ist ein echter Fall.
- **Dismiss**: Es ist ein Fehlalarm.

Ein Status dokumentiert nur, wer wann entschieden hat. Die Bestätigung sperrt selbst nichts: Sperren Sie Produkt oder Tag auf seiner Seite oder lassen Sie dies einen Workflow erledigen.

Filtern Sie mit **Add filter** nach Severity, Status, Signals, Detected date, Asset und Country.

ANALYSEN

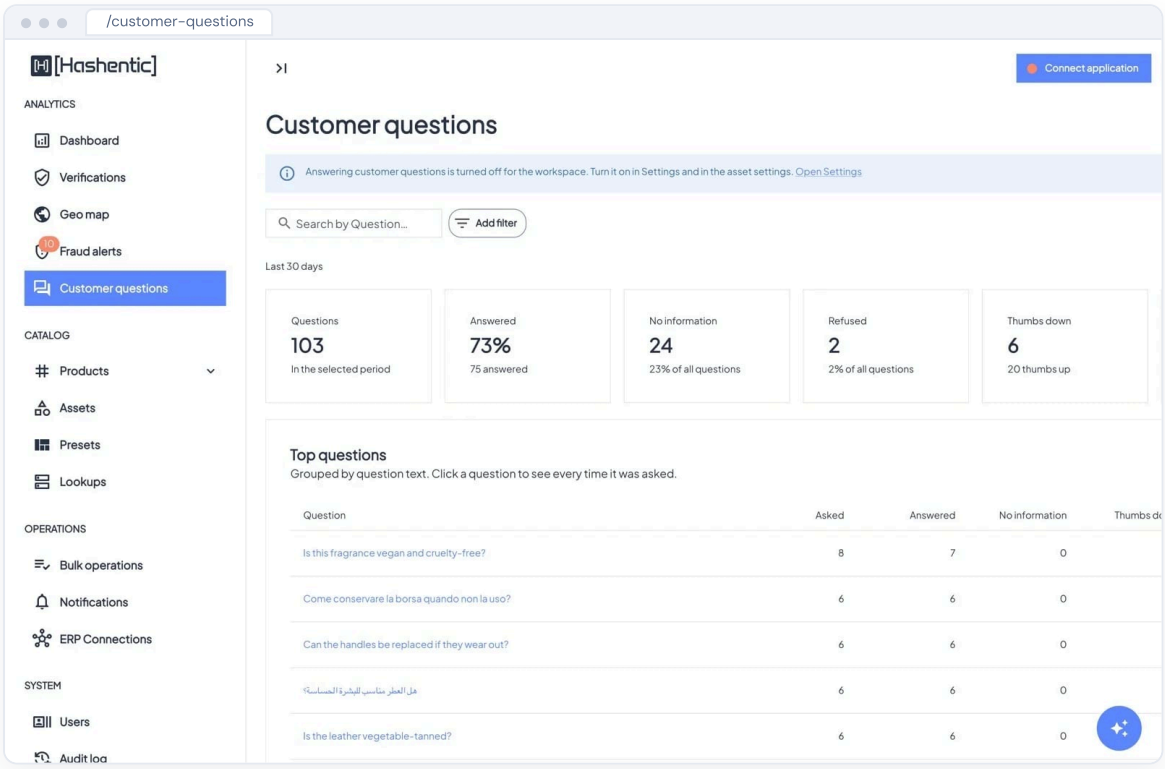
9 Kundenfragen

Kunden können nach der Verifizierung eines echten Produkts auf der Seite einen KI-Assistenten zu Pflege, Garantie oder Inhaltsstoffen befragen. Hier sehen Sie ihre Fragen und die Qualität der Antworten, um Lücken in Ihren Produktinformationen zu schließen.

Menü Analytics → Customer questions

Berechtigung Read customer questions

Lizenz AI + Customer AI



Kundenfragen. Übersichtskacheln filtern die Liste; **Top questions** gruppiert wiederholte Fragen.

- Kacheln für **Questions**, **Answered**, **No information**, **Refused**, **Thumbs down** und **From cache**. Klicken Sie zum Filtern auf eine Kachel.
- **All questions** zeigt Zeitpunkt, Asset, Produkt, Sprache, Status, zitierte Quellen, Kundenfeedback und Land.
- **Top questions** gruppiert identische Fragen mit der Häufigkeit ihrer Stellung und Beantwortung.
- Filtern Sie nach Asset, Zeitraum (7/30/90 Tage oder benutzerdefiniert), Sprache, Status und Feedback.

Status	Bedeutung
Answered	Der Assistent hat aus öffentlichen Produktfeldern, Passdaten und öffentlichen Dokumenten geantwortet.
No information	Ihre Daten enthalten keine Antwort. Ergänzen Sie ein Dokument oder Feld, um die Lücke zu schließen.
Refused	Außerhalb des Aufgabenbereichs: Echtheitsaussagen, sachfremde Themen, personenbezogene Daten oder Versuche, die Regeln des Assistenten zu ändern.
Failed	Der KI-Dienst war vorübergehend nicht verfügbar.

Aktivierung

Zwei Schalter sind erforderlich: **Settings** → **Answer customer questions on the verification page** für den gesamten Arbeitsbereich und **Answer customer questions with AI** im Tab Settings jedes Assets, wo Sie auch einen Begrüßungstext verfassen können. Die Seite ist schreibgeschützt und zeigt Fragen, keine Antworttexte. Antworten werden zur Wiederverwendung zwischengespeichert (beantwortete Fragen für 7 Tage); dies zählt die Kachel *From cache*.

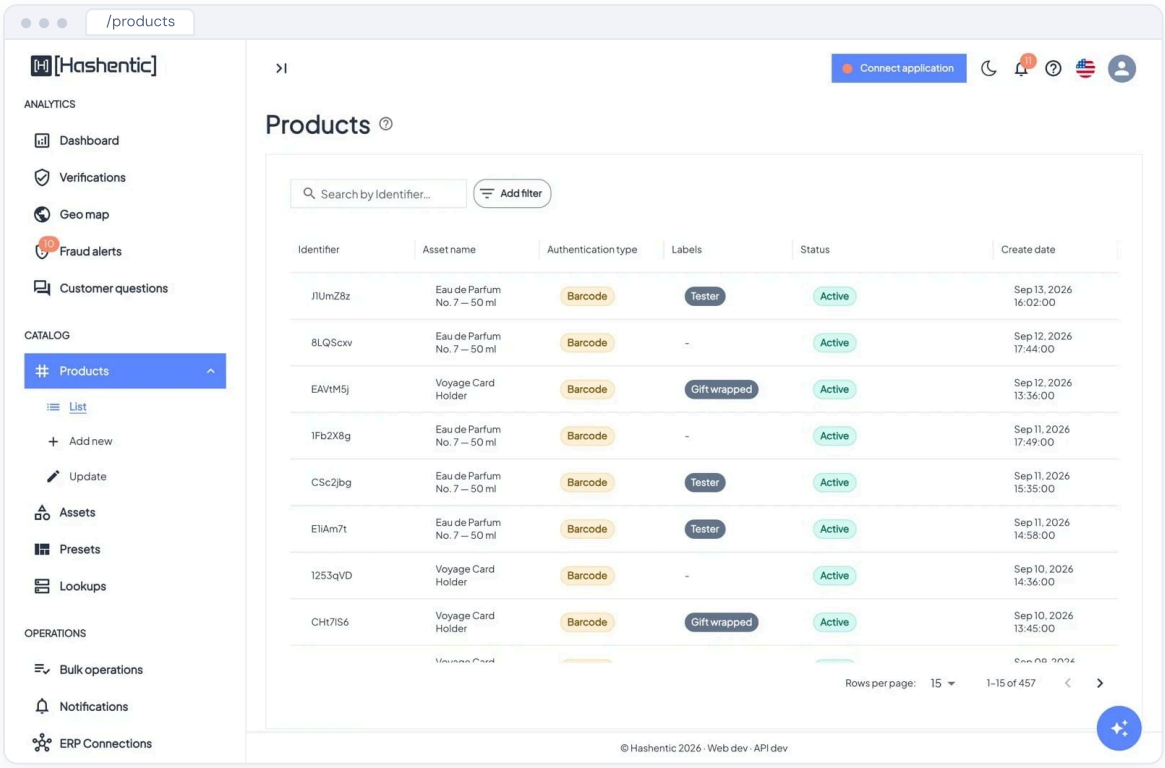
KATALOG

10 Produkte

Alle von Ihnen ausgegebenen gekennzeichneten Artikel. Finden Sie Produkte in Sekunden, sehen Sie Scans und Verlauf, bearbeiten Sie Daten, drucken Sie Codes oder sperren Sie Produkte.

Menü Catalog → Products → List

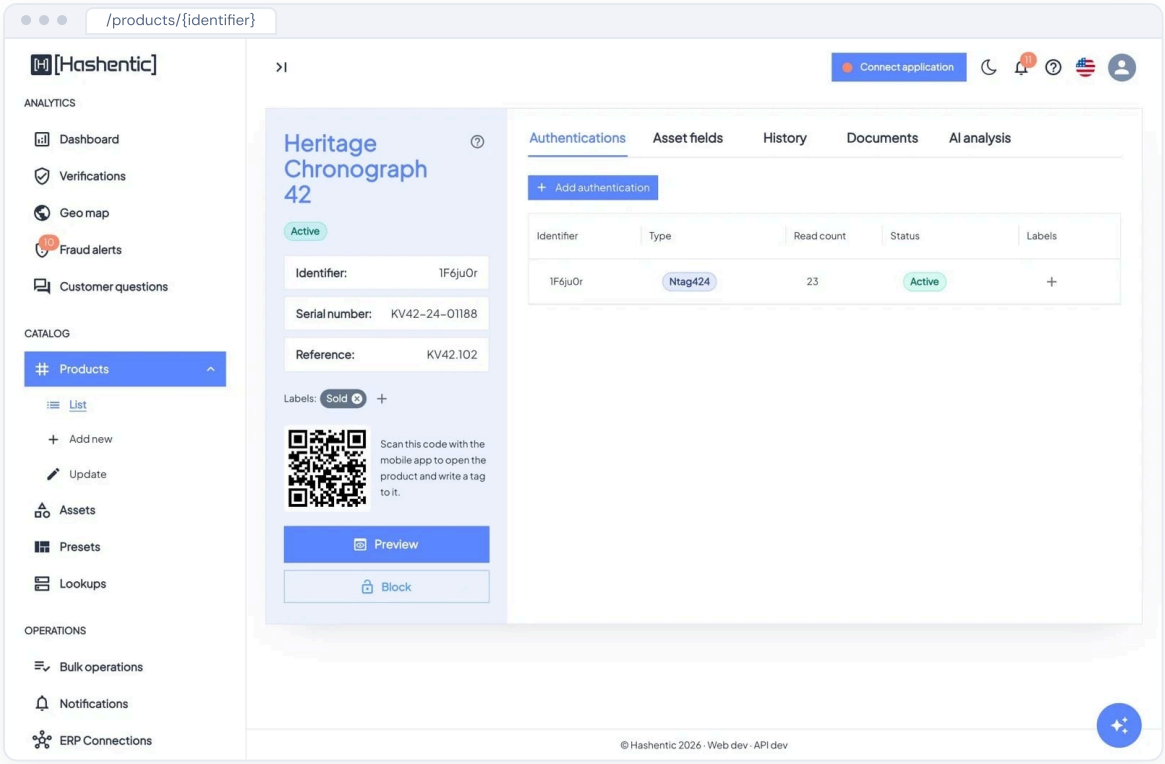
Berechtigung Read products



Produkte. Spalten: Identifier, Asset name, Authentication type, Labels, Status und Create date. Mit *Show in grid* markierte Felder erscheinen als zusätzliche Spalten im Products-Tab des Assets.

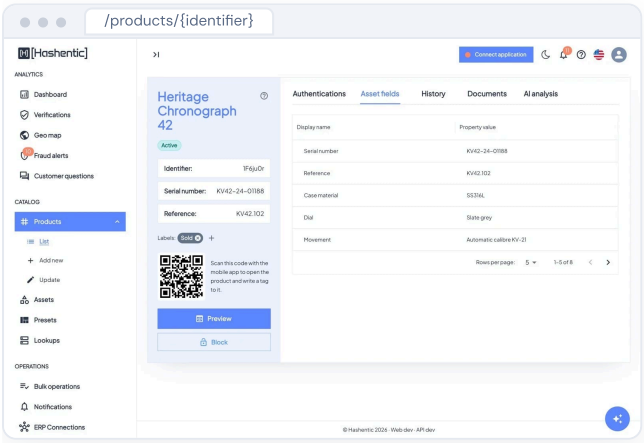
Suchen Sie nach der Kennung oder nutzen Sie **Add filter** für Identifier, UID, Authentication type, Labels, Deleted, Blocked und Create date. Unter **Products** finden Sie außerdem **Add new** (Produkte anlegen und kennzeichnen, siehe Kapitel 16) und **Update** (Produkte zum Bearbeiten scannen, einzeln oder gesammelt).

Die Produktseite

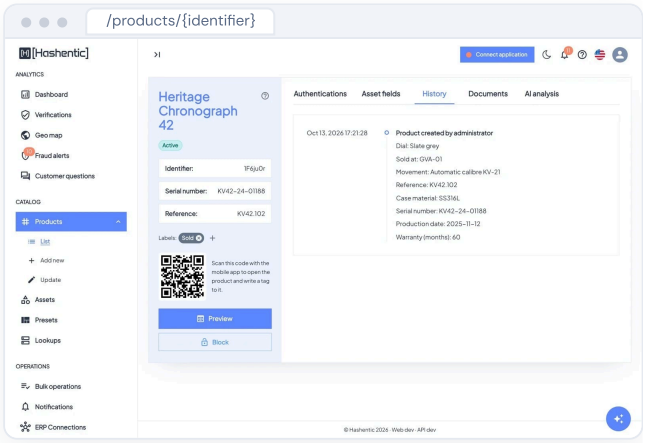


Produktseite. Links: Status, zentrale Werte, Labels und ein QR-Code für die mobile App. Rechts: Tabs.

> **Sperren oder löschen**
>
> Sperren Sie ein Produkt bei Diebstahl, Rückruf oder Kopierverdacht: Kunden sehen beim Scan die Seite für ungültige Scans; Sie können es später entsperren. Im Tab Authentications können Sie auch einen einzelnen Tag sperren, während die übrigen Tags weiter funktionieren. Gesperrte NTAG-215-Produkte lassen sich nicht über den Administrationsbereich löschen.



Tab Asset fields: die Produktwerte.



Tab History: jede Änderung mit Urheber und Zeitpunkt.

Tabs

- **Authentications**: Tags und Codes des Produkts mit Typ, Leseanzahl, Status und Labels. Ergänzen Sie mit **Add authentication** eine weitere Authentifizierung; sperren, entsperren oder entfernen Sie einzelne, laden Sie Barcodes herunter oder weisen Sie eine eigene Seitenvorlage zu.
- **Asset fields**: die Produktwerte.

Aktionen

- **Preview** zeigt die Verifizierungsseite genau so, wie Kunden sie sehen.
- **Edit** ändert Werte von Feldern, die Aktualisierungen erlauben.

- **History**: wer das Produkt angelegt und geändert hat und was geändert wurde.
- **Documents**: Dateien für diesen Artikel (Zertifikat, Wartungsnachweis).
- **AI analysis**: Fragen zu den Scans dieses Produkts stellen (Kapitel 19).

- Bei Produkten mit sicheren NFC-Tags erscheinen Edit, Block und Delete nach dem Einlesen des Tags (**Products** → **Update**) oder wenn das Asset ungeschützte Verwaltung erlaubt. Einzelne Tags können im Tab Authentications jederzeit gesperrt werden.
- **Download** exportiert den Barcode als PDF, CSV, XLSX oder TXT.
- **Block** / **Unblock**: Jede Verifizierung eines gesperrten Produkts schlägt fehl.
- **Delete** nimmt das Produkt aus der Nutzung; es bleibt als gelöscht in den Datensätzen erhalten.
- **QR for the mobile app** öffnet das Produkt in der mobilen App, etwa um einen Tag dafür zu beschreiben.

KATALOG

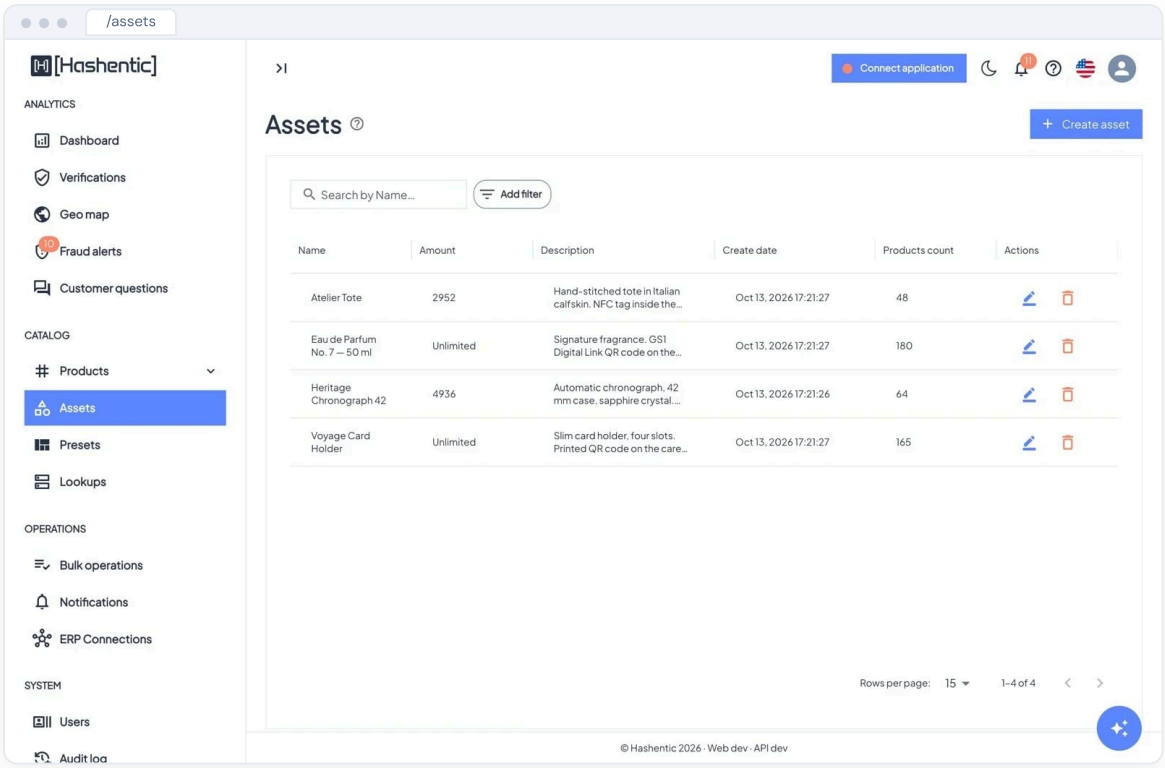
11 Assets und Felder

Ein Asset ist eine Produktlinie: die Vorlage für jeden ihrer Artikel. Seine Seite vereint Felder, Verifizierungsseite, Dokumente, Labels, Formulare, Workflows und Betrugsregeln der Linie.

Menü Catalog → Assets

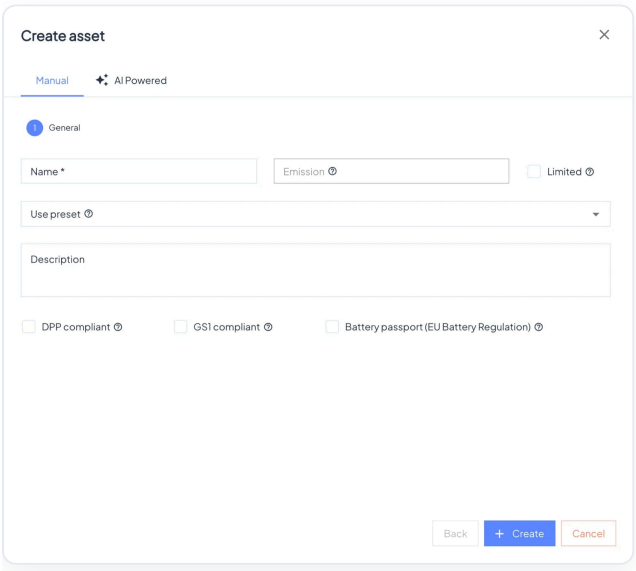
Berechtigung Read / Write / Delete assets

Limit Asset-Anzahl Ihrer Lizenz



Assets. Amount zeigt, wie viele Produkte noch angelegt werden dürfen ("Unlimited" für unbegrenzte Linien), Products zählt vorhandene Produkte.

Ein Asset erstellen



Create asset: manuell oder KI-gestützt.

Create asset öffnet ein kurzes Formular: **Name** (mindestens 4 Zeichen), optional **Amount** mit **Limited** zur Begrenzung der Produktanzahl, optional ein **Preset** zum Übernehmen von Feldern und Vorlage sowie **Description**.

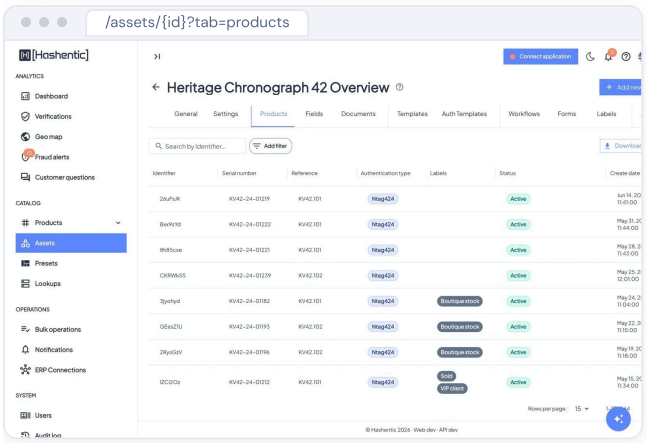
Drei Optionen ergänzen Konformitätsschritte:

- **GS1 compliant**: GTIN, Markenname, Handelsartikelbeschreibung, Nettoinhalt und Zielmarkt; **Find product by GTIN** füllt diese aus.
- **DPP compliant**: Daten für den Digitalen Produktpass, Wirtschaftsakteur sowie Informationen zu Kreislauffähigkeit und Nachhaltigkeit.
- **Battery passport (EU Battery Regulation)**: ergänzt Batteriepassfelder.

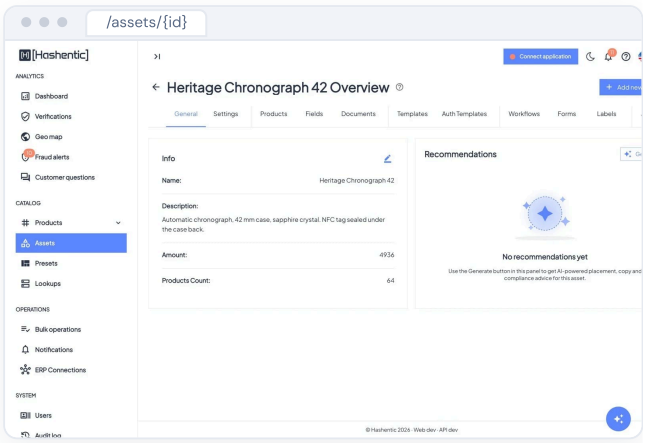
Der Tab **AI Powered** entwirft anhand einer kurzen Produktbeschreibung Felder und eine Seitenvorlage.

Die Asset-Seite

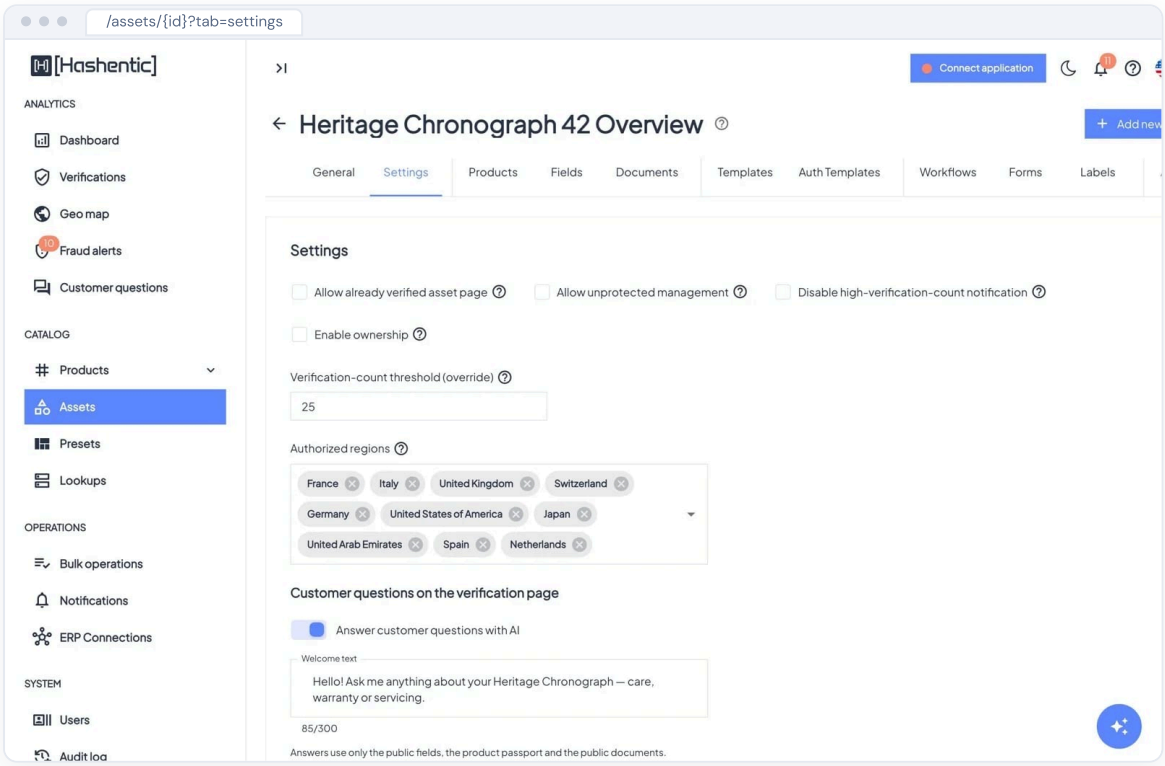
Tabs: **General** · **Settings** · **Products** · **Fields** · **Documents** · **Templates** · **Auth templates** · **Workflows** · **Forms** · **Labels** · **AI analysis**. Die Schaltfläche **Add new product** oben startet die Kennzeichnung mit bereits ausgewähltem Asset.



Tab Products: Artikel dieser Linie, Filter und **Download barcodes** für die gefilterte Auswahl.



Tab General: Name, Beschreibung, Anzahl und KI-**Recommendations** zum Schutz der Linie.

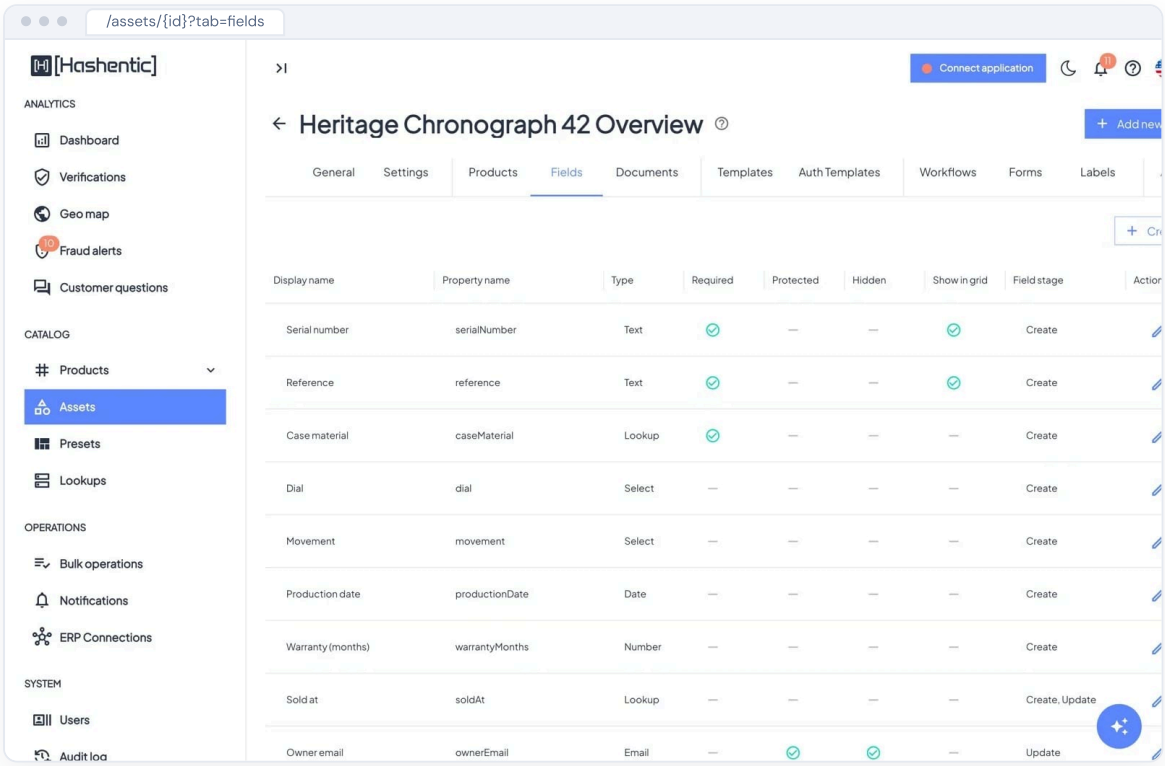


Tab Settings. Authorized regions steuert die Graumarkterkennung; der Bereich für Kundenfragen aktiviert den KI-Assistenten für diese Linie.

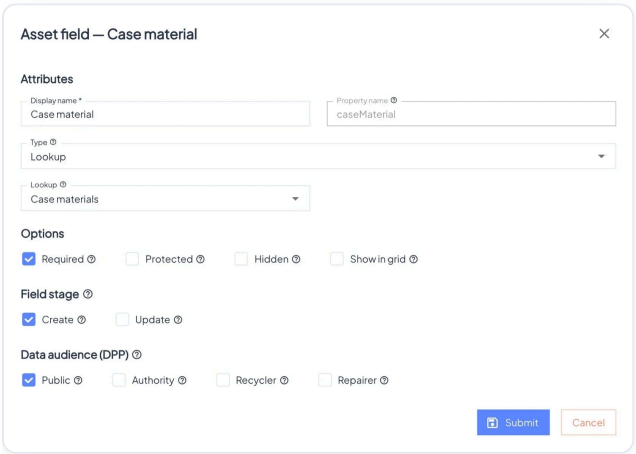
Asset-Einstellung	Wirkung
Allow already verified asset page	Beim erneuten Öffnen eines sicheren Tag-Links erscheint eine gestaltete Seite mit dem Hinweis "Product is not verified: this link has already been used." anstelle der Fehlerseite. Hilfreich, wenn Kunden Produktinformationen erneut aufrufen.
Allow unprotected management	Mitarbeiter können Produkte mit sicheren NFC-Tags ohne Einlesen des Tags aktualisieren, sperren oder löschen. Das Asset wird auch für Massenaktualisierungen per Abfrage verfügbar.
Disable high-verification-count notification / threshold	Steuert die Benachrichtigung bei ungewöhnlich häufigen Scans eines Tags.

Asset-Einstellung	Wirkung
Authorized regions	Verkaufsländer dieser Linie. Wiederholte echte Scans außerhalb lösen einen *Gray market*-Alarm aus.
Answer customer questions with AI · Welcome text	KI-Assistent auf der Verifizierungsseite dieser Linie und sein Begrüßungstext.
Enable ownership	Erfasst Produkteigentum (mit der Lizenzfunktion Product ownership).

Felder



Tab Fields. Daten, die jedes Produkt der Linie enthält.



Feldeinstellungen für ein Lookup-Feld.

Typen: Text, Email, Number, Select (eigene Auswahlliste), Lookup (Werte aus einem Lookup), Date und Checkbox, jeweils mit eigenen Prüfungen (Länge, Muster, Minimum/Maximum, nur vergangene oder zukünftige Daten).

Optionen

- **Required**: muss ausgefüllt sein.

- **Protected** : verschlüsselt gespeichert und von der Suche ausgeschlossen. Für personenbezogene Daten wie die E-Mail-Adresse eines Eigentümers. Wer das Produkt öffnen darf, sieht den echten Wert, ebenso auf Barcodes; der Workflow-Verlauf zeigt •••. Ein geschütztes Feld erscheint nie auf der Verifizierungsseite oder in KI-Antworten und kann daher nicht zugleich öffentlich sein: Aktivieren Sie **Hidden** oder entfernen Sie die Zielgruppe **Public** . Wenn Sie **Protected** bei einem öffentlichen Feld aktivieren, geschieht das automatisch; ein geschütztes Feld, das noch öffentlich ist, lässt sich nicht speichern. Die Verschlüsselung gilt für Werte, die nach dem Aktivieren gespeichert werden; bereits erfasste Werte, auch auf der Blockchain, bleiben unverändert. Geschützte Felder können nicht zum Filtern von Produkten oder zum Eingrenzen von Workflows verwendet werden.
- **Hidden** : auf der Standardseite nicht für Kunden sichtbar.
- **Show in grid** : als Spalte in der Produktliste des Assets.

Field stage: **Create** -Felder werden beim Erstellen des Produkts ausgefüllt; **Update** -Felder können später geändert werden (etwa "Verkaufsort"). **Data audience** legt fest, welche Partner des Digitalen Produktpasses (Behörde, Recycler, Reparaturbetrieb) ein Feld sehen dürfen.

> ! **Sobald Produkte vorhanden sind**
>
> Der Eigenschaftsname eines Feldes wird beim Anlegen festgelegt. Sobald ein Asset Produkte enthält, können Felder nicht mehr gelöscht werden (Ergänzen und Bearbeiten bleiben möglich). Planen Sie die Struktur zunächst mit einem Test-Asset oder speichern Sie sie als Preset.

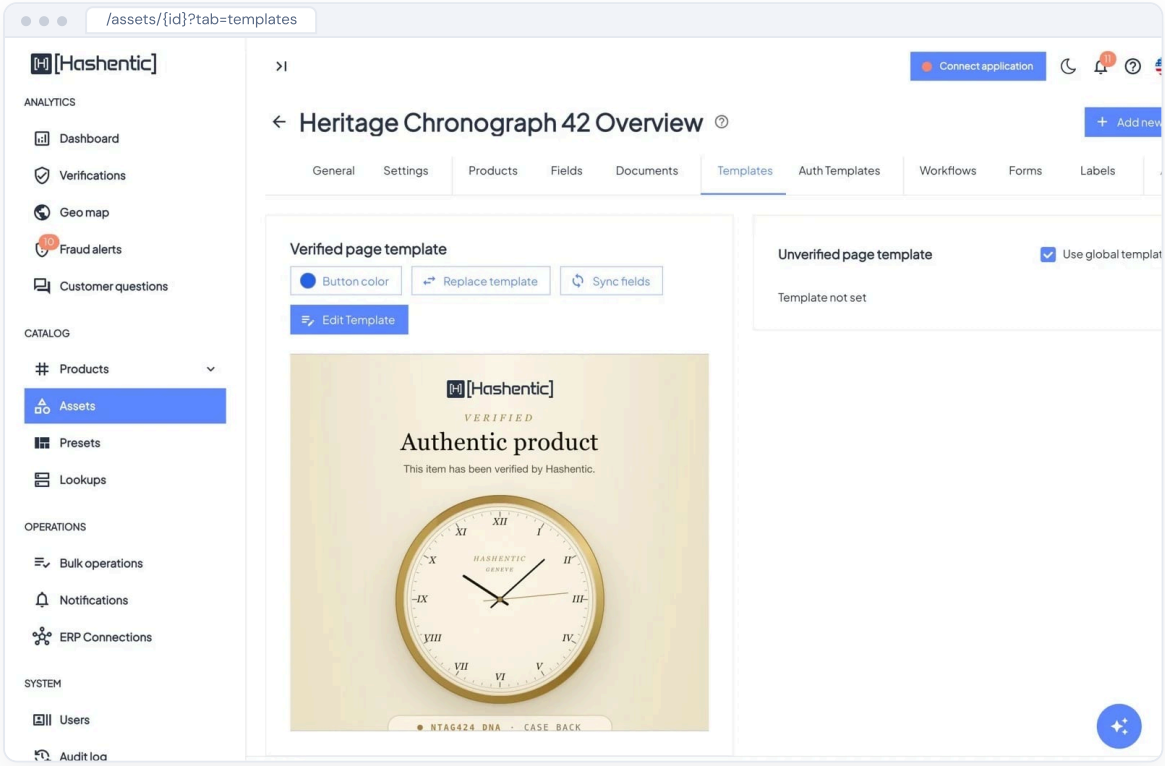
KATALOG

12 Vorlagen für Verifizierungsseiten

Die Seite nach dem Scan ist ein Kontaktpunkt mit Ihrer Marke. Jedes Asset bestimmt ihre Gestaltung für erfolgreiche und fehlgeschlagene Verifizierungen.

Ort Asset → Tab Templates; Settings → Unverified page template

Berechtigung Write assets



Tab Templates. Seite für gültige Scans links, für ungültige rechts.

Möglichkeiten der Seitengestaltung

Vorlagengalerie

Über 60 fertige Designs, von minimalen und redaktionellen Stilen bis zu Branchenseiten für Uhren, Taschen, Kosmetik, Wein, Pharma oder Batterien sowie Layouts für Digitale Produktpässe. Nach Stil, Anwendung und Layout filtern, hell oder dunkel ansehen, Felder auswählen und anwenden.

Blockeditor

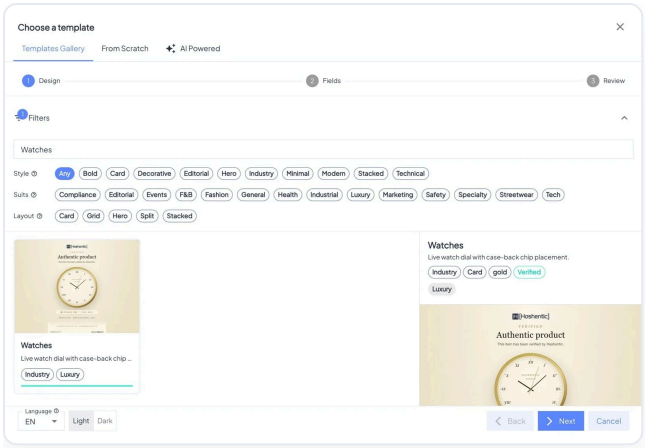
Ein Drag-and-drop-Editor (**Edit Template**) mit Überschriften, Text, Bildern, Schaltflächen, Spalten und Trennlinien sowie Desktop- und Mobilvorschau.

Eigenes HTML

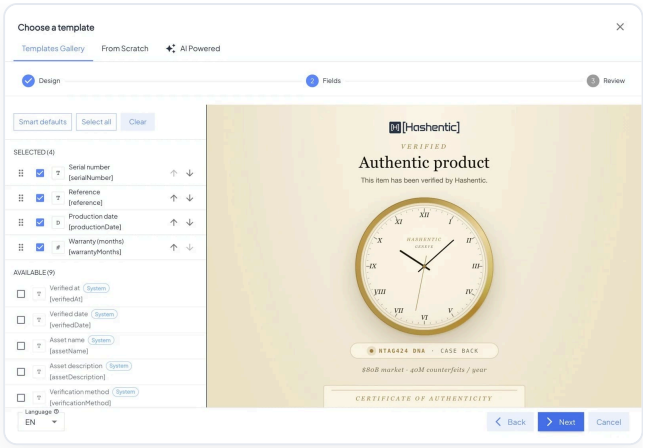
Eigenes HTML und CSS mit Platzhaltern wie **[AssetName]**, **[VerifiedAt]** oder Feldern wie **[serialNumber]** (siehe Anhang B).

Externe Website · KI-gestützt

Seite Ihrer eigenen Website anzeigen oder eine Vorlage für das Asset von KI erzeugen lassen. Auch das Kopieren der Vorlage eines anderen Assets ist möglich.



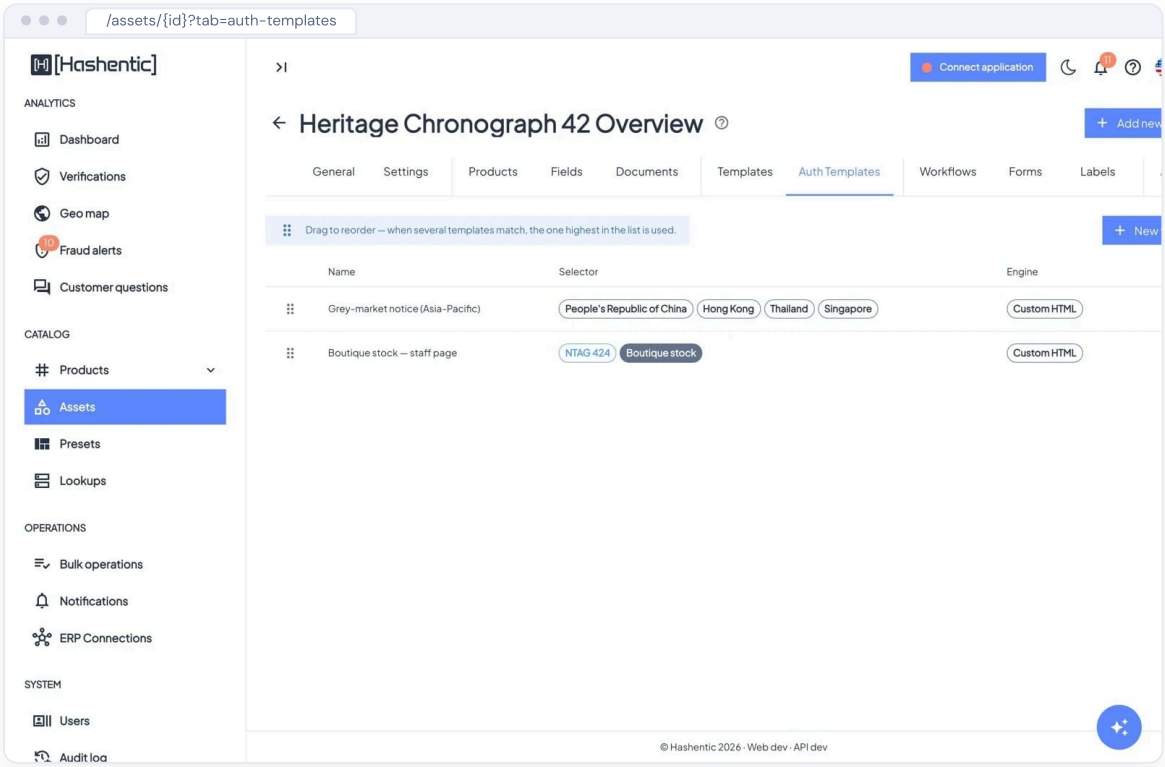
Choose a template: Design auswählen und Vorschau öffnen.



Schritt Fields: sichtbare Felder auswählen und anordnen.

Weitere Steuerungsmöglichkeiten

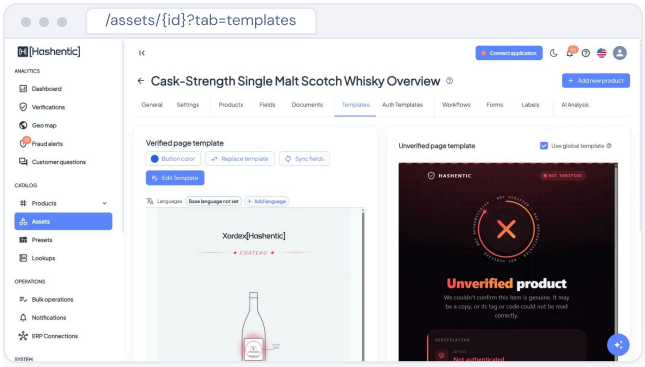
- **Button color**: Farbe der KI-Assistenten- und Dokumentenschaltflächen; ohne Angabe wird Ihre Markenfarbe verwendet.
- **Unverified page template**: je Asset oder **Use global template** aus Settings; Fehlerseitenregeln können sie bei bestimmten Fehlern ersetzen.
- **Sync fields**: Vorlage nach Ergänzung oder Umbenennung von Feldern aktualisieren.
- **Auth templates**: alternative Seiten für gültige Scans, ausgewählt nach Tag-Typ, Produktlabel oder Scanland, etwa ein Hinweis für Scans außerhalb Ihrer Märkte.



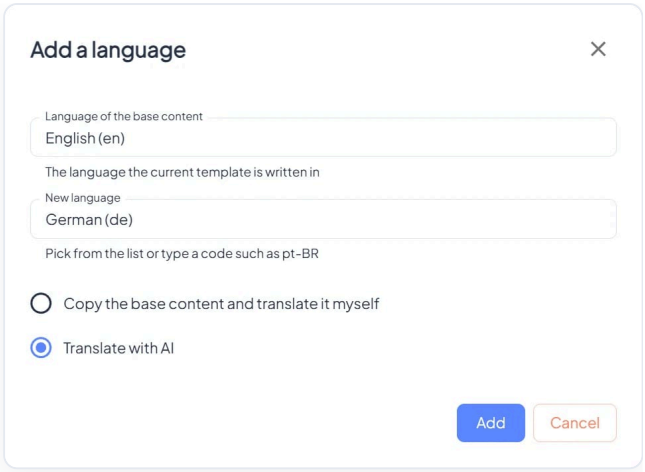
Auth-Vorlagen. Treffen mehrere zu, gilt die oberste; ziehen Sie Zeilen zum Umordnen.

Sprachen

Jede Seitenvorlage kann andere Sprachversionen haben: gültige und ungültige Seite des Assets, jede Auth-Vorlage, jede Fehlerseitenregel und die globale ungültige Seite in Settings. Besucher sehen die bevorzugte Browsersprache. Fehlt diese Version, erscheint der Basisinhalt.



Languages unter der Vorlage: Basissprache und **Add language**.



Sprache hinzufügen: einmalig die Basissprache, dann neue Sprache und KI-Übersetzung oder eine andere Vorlage.

- Die Leiste **Languages** unter einer Vorlage zeigt Basissprache und jede Version. **Add language** fragt einmal nach **Language of the base content**, dann nach **New language**: aus der Liste wählen oder einen Code wie `pt-BR` eingeben.
- **Translate the base template with AI** übersetzt Texte und erhält Layout, Bilder, Links und Platzhalter; nicht übersetzbare Inhalte bleiben wie in der Basis. KI-Übersetzung ist für Vorlagen mit externer Website nicht verfügbar.
- **Choose a different template** gibt der Sprache ein eigenes Design: **Choose a template** öffnet dieselbe Galerie wie für die Basisvorlage, einschließlich der Optionen, bei null zu beginnen oder die KI eine Vorlage erstellen zu lassen. Eine Sprache kann sogar eine andere Vorlagenart als die Basis verwenden, zum Beispiel eine externe Website in dieser Sprache.
- Öffnen Sie eine Sprache, um sie mit **Edit** zu bearbeiten, mit **Translate the base template with AI** zu erneuern (Ihre Änderungen in dieser Sprache werden ersetzt), ihr mit **Replace template** ein neues Design zu geben oder sie mit **Delete language** zu entfernen.
- Bis zu 10 Sprachen pro Vorlage. Die Schaltflächenfarbe ist in allen Sprachen gleich.
- Regionale Browsersprachen fallen auf die Hauptsprache zurück: *pl-PL* sieht *pl*, *de-AT* sieht *de*.

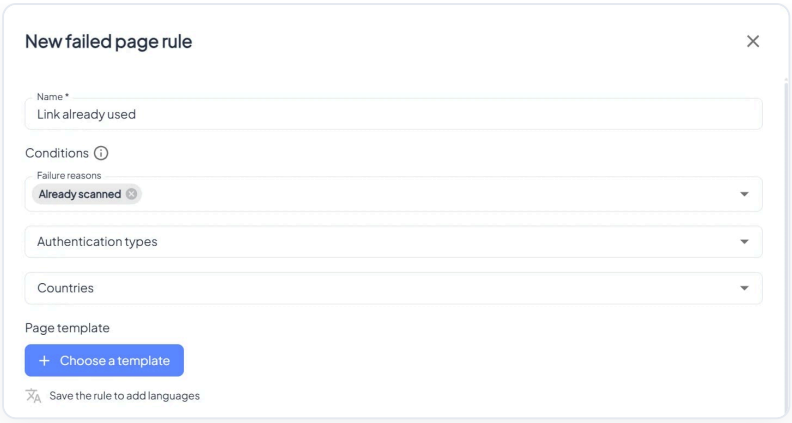
> **Übersetzungen beginnen mit der gespeicherten Vorlage**
>
> Speichern Sie Änderungen vor dem Hinzufügen oder erneuten Übersetzen einer Sprache. Speichern Sie bei Auth-Vorlagen und Fehlerseitenregeln zuerst die Regel. Spätere Änderungen des Basisinhalts werden nicht in Sprachversionen kopiert: Aktualisieren Sie jede mit **Translate the base template with AI** oder manuell.

Regeln für Fehlerseiten

Die Seite für ungültige Scans kann nach Fehlergrund, Tag-/Codetyp und Scanland variieren. **Failed page rules** stehen unterhalb der Auth-Vorlagen im Tab **Auth templates** des Assets; Regeln für alle Produkte stehen unter System → Settings unterhalb der globalen ungültigen Seitenvorlage.

Eine Regel kann drei Bedingungen prüfen:

- **Failure reasons** (Anhang A):
  - *Already scanned*: Ein einmaliger NFC-Link wurde erneut geöffnet.
  - *Blocked or withdrawn*: Das Produkt oder dieser Tag ist gesperrt.
  - *Internal use only*: Die Produktlinie ist auf interne Prüfungen beschränkt.
  - *Authentication failed*: jeder andere Grund, etwa unbekannter Code, falsche Signatur oder abweichender Zähler.
- **Authentication types**: Typ des Tags oder Codes hinter dem Link, auch bei nie registrierten Tags bekannt.
- **Countries**: aus der Internetadresse des scannenden Geräts; benötigt die Lizenzfunktion *Geolocation analytics*.



Neue Fehlerseitenregel: Name, Bedingungen und anzuzeigende Seite.

Regeln verwenden:

- **New rule** fragt nach **Name**, **Conditions** und **Page template**. Alle Bedingungen müssen zutreffen; eine leere Bedingung passt auf alles (*Any failure*, *All*).
- Die erste passende Regel gilt: Ziehen Sie Zeilen zum Sortieren und öffnen Sie Regeln zum Bearbeiten.
- Die Seite jeder Regel kann eigene Sprachen haben.
- Produktlabels werden nicht angeboten: Ein fehlgeschlagener Scan kann seine Produktzugehörigkeit nicht beweisen.

Ein fehlgeschlagener Scan zeigt den ersten zutreffenden Eintrag:

1. Fehlerseitenregeln des Assets, erster Treffer.
2. Eigene Vorlage für ungültige Scans des Assets.
3. Fehlerseitenregeln in Settings, erster Treffer.
4. Vorlage für ungültige Scans in Settings.
5. Integrierte Seite in der Besuchersprache.

Ist **Allow already verified asset page** aktiviert, zeigen wiederholte Scans sicherer Tags weiterhin die gestaltete Produktseite mit Hinweis statt einer Seite für *Already scanned*.

KATALOG

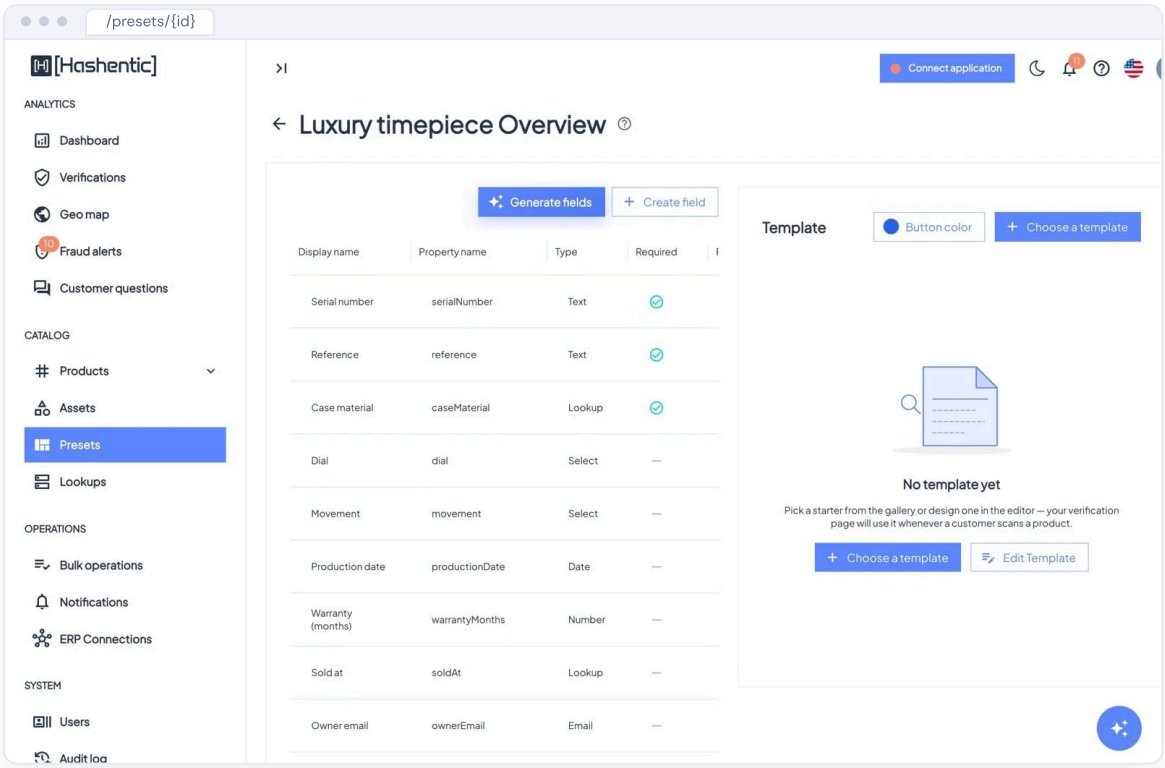
13 Presets und Lookups

Zwei Werkzeuge für einen konsistenten großen Katalog: Presets verwenden Strukturen wieder, Lookups Werte.

Presets

Menü Catalog → Presets **Berechtigung** Read / Write presets

Ein Preset kombiniert Felder und eine Seitenvorlage. Erstellen Sie eines mit **Create preset**, ergänzen Sie Felder und wählen Sie eine Vorlage wie bei einem Asset. Wählen Sie beim Anlegen eines Assets das Preset unter **Use preset**; es beginnt dann mit denselben Feldern und derselben Seite. System-Presets stellt Hashentic bereit; Benutzer-Presets gehören Ihnen.



Ein Preset für Luxusuhren: Felder links, Vorlage rechts.

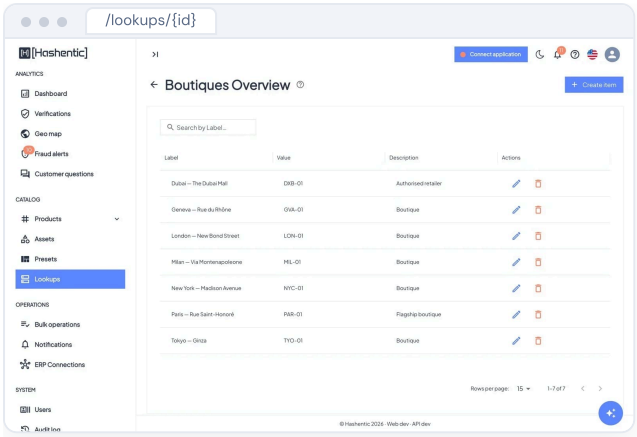
Lookups

Menü Catalog → Lookups **Berechtigung** Read / Write lookups

Ein Lookup ist eine benannte Liste, etwa für Materialien, Boutiquen oder Märkte. Jeder Eintrag hat **Value** (am Produkt gespeichert), **Label** (für Menschen angezeigt) und eine Beschreibung.

Ergänzen Sie Einträge einzeln (**Single mode**) oder importieren Sie eine CSV- oder Excel-Datei (**Multiple mode**, mit der Lizenzfunktion Bulk write und der Berechtigung Write products). Ordnen Sie deren Spalten Wert, Bezeichnung und Beschreibung zu. Aktivieren Sie **Override**, um die gesamte Liste zu ersetzen.

Verwenden Sie den Lookup anschließend in beliebig vielen Lookup-Feldern.



Ein Lookup für Boutiquen: Bezeichnung, Wert und Beschreibung jedes Eintrags.

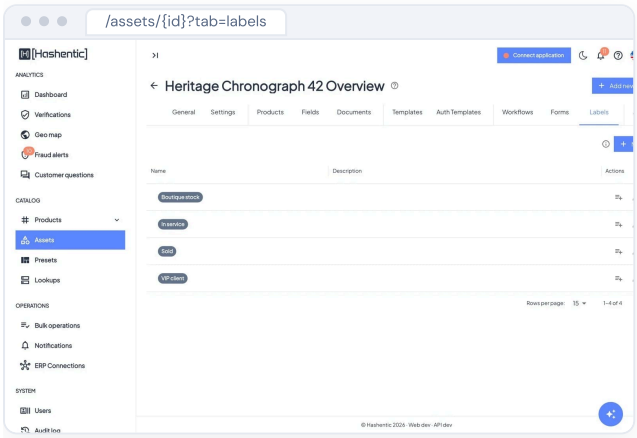
KATALOG

14 Labels und Formulare

Labels kennzeichnen den Zustand von Produkten und Tags; über Formulare senden Kunden Ihnen Informationen von der Verifizierungsseite.

Labels

Ort Asset → Tab Labels **Limit** 15 Labels pro Asset



Labels der Uhrenlinie.

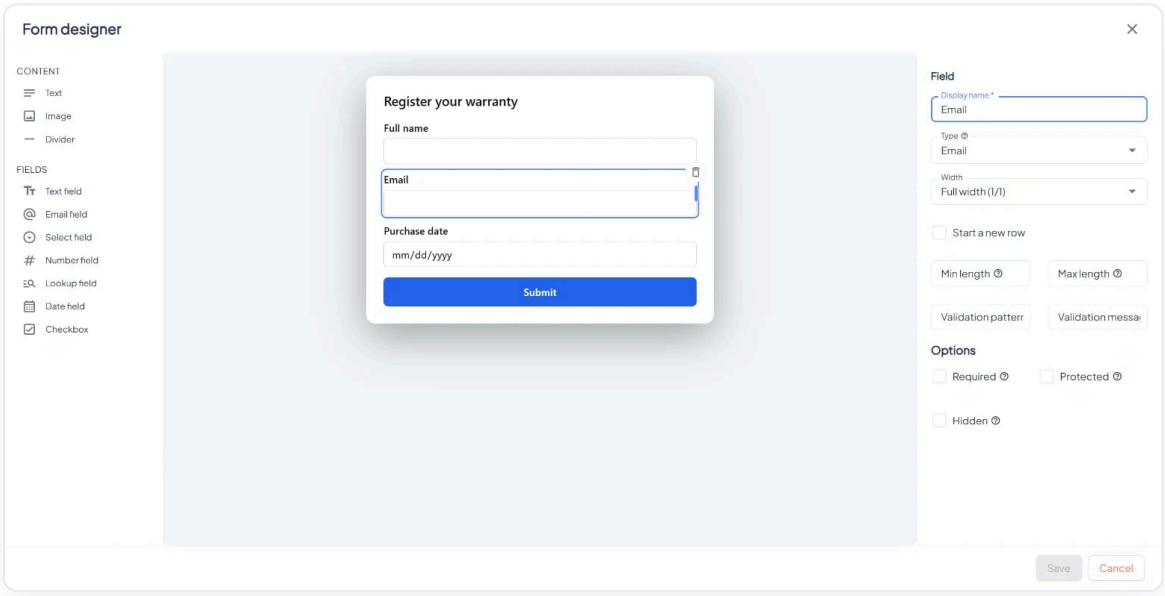
Erstellen Sie Labels mit **New label** (Name, Farbe, Beschreibung), etwa *Boutique stock*, *Sold*, *In service*. Wenden Sie sie auf der Produktseite, gesammelt mit **Bulk apply / remove** oder aus Workflows an.

Labels können eine andere Verifizierungsseite auswählen (Auth-Vorlagen), die Sichtbarkeit von Formularen bestimmen, den Geltungsbereich eines Workflows begrenzen und Produktlisten filtern.

Formulare

Ort Asset → Tab Forms **Lizenz** Asset forms

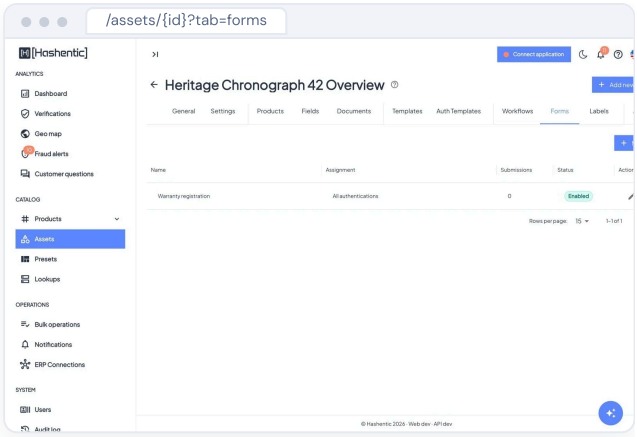
Formulare erscheinen nach einem Scan auf der Verifizierungsseite: Garantieregistrierung, Newsletter-Anmeldung, Reparaturanfragen. **New form** öffnet den Formulardesigner mit Text-, Bild- und Trennblöcken, allen Feldtypen und einem optionalen DSGVO-Einwilligungsfeld.



Formulardesigner. Blöcke links, das Formular live in der Mitte, Einstellungen rechts.

- **Show this form to**: alle Authentifizierungen, ein Tag-Typ oder Produkte mit einem bestimmten Label.

- **Allow only one submission per authentication** und **Allow the customer to skip this form**: einmaliges Einsenden und Überspringen erlauben.
- **Show after delay (ms)** lässt zuerst die Seite laden.
- **Submissions**: alle Antworten mit Produkt und Datum einsehen und mit **Download submissions (CSV)** herunterladen.
- Eine Einsendung kann einen Workflow auslösen (*On form submit*).



Tab Forms mit dem Formular zur Garantieregistrierung.

Lizenz AI **Generate with AI** unten im Formular-Designer erstellt ein Formular aus einer Beschreibung wie "Garantieregistrierung mit Name, E-Mail, Kaufdatum und Geschäft". Felder mit personenbezogenen Daten werden als **Protected** markiert und mit einem Einwilligungsfeld geliefert. Prüfen Sie das Ergebnis im Designer, bevor Sie speichern.

> **Geschützte Felder**
>
> Aktivieren Sie **Protected** bei Feldern, die personenbezogene Daten erfassen, etwa eine E-Mail-Adresse oder Telefonnummer. Hashentic speichert den übermittelten Wert verschlüsselt. Die Liste Submissions und der CSV-Download zeigen allen, die sie öffnen dürfen, den echten Wert. Workflows können den Wert weiterhin per E-Mail oder HTTP-Anfrage senden. Ausführungsverlauf und Benachrichtigungen zeigen ••• statt des Werts, und ein Workflow kann ihn nur in ein geschütztes Produktfeld kopieren. Die Einstellung gilt für neue Einsendungen: Antworten, die vor dem Aktivieren gespeichert wurden, bleiben unverschlüsselt.

AUTOMATISIERUNG

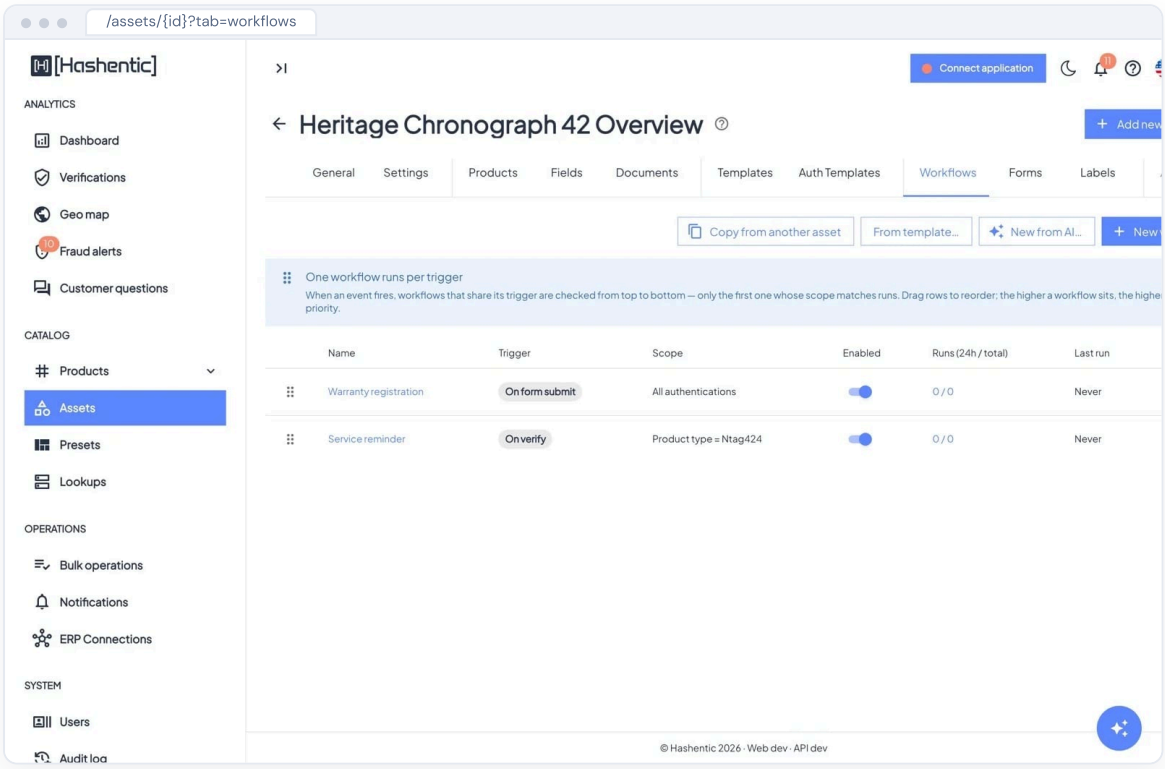
15 Automatisierte Workflows

Workflows reagieren auf Produktereignisse, ohne dass jemand den Bildschirm beobachten muss: geklonte Tags sperren, Produkte bei Garantieregistrierung kennzeichnen, das Team vor wiederholten Scans warnen oder Ihr CRM informieren.

Ort Asset → Tab Workflows

Berechtigung Read / Write workflows

Lizenz Workflows



Workflows eines Assets. Auslöser, Geltungsbereich, Ein/Aus, Durchläufe der letzten 24 Stunden und insgesamt sowie letzter Durchlauf.

Bausteine

Auslöser

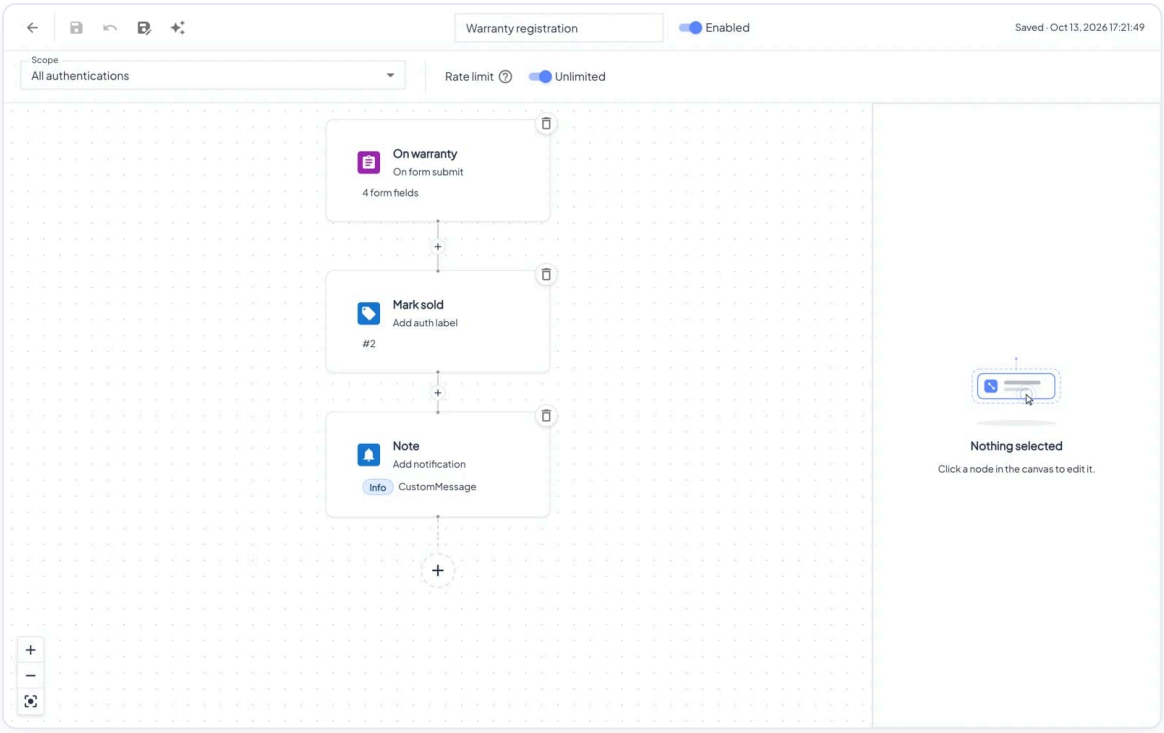
On verify (jeder echte Scan) · On form submit · On product blocked · On product create · On external webhook · On fraud detected (mit Mindestschweregrad).

Aktionen

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

Logik

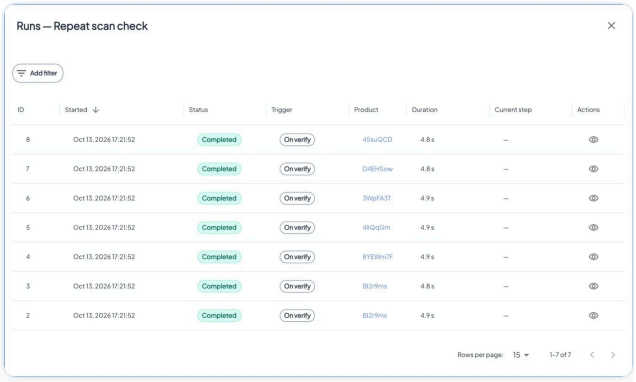
Bedingungen mit AND/OR-Gruppen für Felder, Land, Betriebssystem, Tag-Typ, Scananzahl, Entfernung zum letzten Scan, Tageszeit, Produktalter oder Labels, mit Dann-/Sonst-Zweigen. Delay wartet Minuten, Stunden oder Tage.



Der Workflow-Editor. Die Arbeitsfläche zeigt Auslöser und Schritte; `+` an einer Verbindung fügt einen Schritt ein. Klicken Sie auf einen Schritt, um ihn rechts zu bearbeiten.

Gut zu wissen

- **Pro Auslöser läuft ein Workflow.** Teilen mehrere Workflows eines Assets einen Auslöser, läuft der erste (oberste) mit passendem **Geltungsbereich**. Ziehen Sie Zeilen zum Sortieren.
- **Scope** beschränkt einen Workflow auf Tag-Typ oder Kategorie, einen Feldwert, bestimmte Tags oder Tags mit einem Label.
- Jedes Speichern erzeugt eine neue **Version**; frühere können angezeigt und wiederhergestellt werden.
- Beginnen Sie mit **From template…** (etwa *Anti-counterfeit: block on second scan*), kopieren Sie von einem anderen Asset oder beschreiben Sie den Workflow unter **New from AI…**.
- In Textfeldern fügt die **Token-Auswahl** Werte wie Scanland, Produkt-ID oder ein eigenes Feld ein.



Durchläufe öffnen Sie über ihre Anzahl. Jeder zeigt Status, Produkt und Ergebnis jedes Schritts.

> **Andere Systeme verbinden**
>
> Ein Workflow mit **On external webhook** erhält eine eigene URL und ein Geheimnis: Ihr System signiert jede Anfrage damit, und Hashentic startet den Workflow für das Produkt aus der Nutzlast. Schritte vom Typ **HTTP request** rufen Ihre Systeme auf; ihre Adressen müssen unter **Settings** → **Workflows URL allowlist** stehen. **Integration guide** im Menü erklärt beides.

BETRIEB

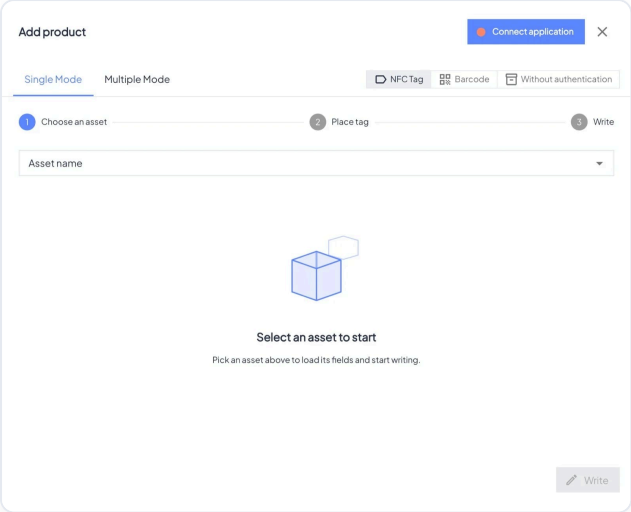
16 Tags beschreiben und Barcodes drucken

Produkte anlegen und authentifizieren erfolgt in einem Dialog: **Products → Add new**. NFC-Tags werden über ein USB-Lesegerät mit dem Desktop-Dienstprogramm beschrieben; Barcodes werden sofort erzeugt und zum Drucken exportiert.

Menü Catalog → Products → Add new

Berechtigung Write products

Lizenz Bulk write für Multiple mode



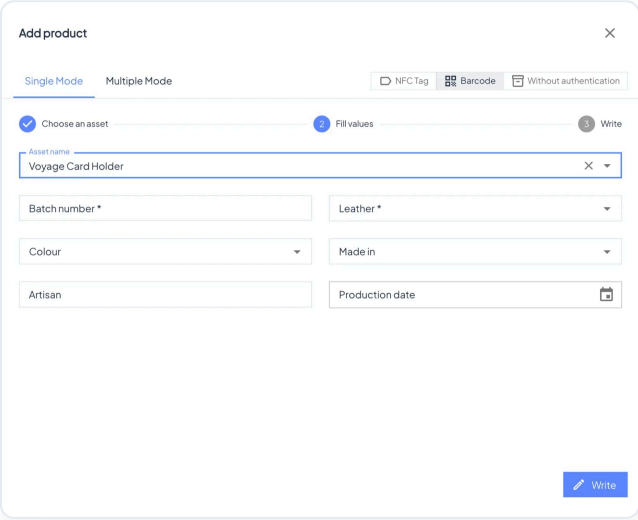
Add product, NFC Tag, Single mode. Die obere Schaltfläche zeigt die Verbindung zum Desktop-Dienstprogramm.

Auswählen, was erstellt wird

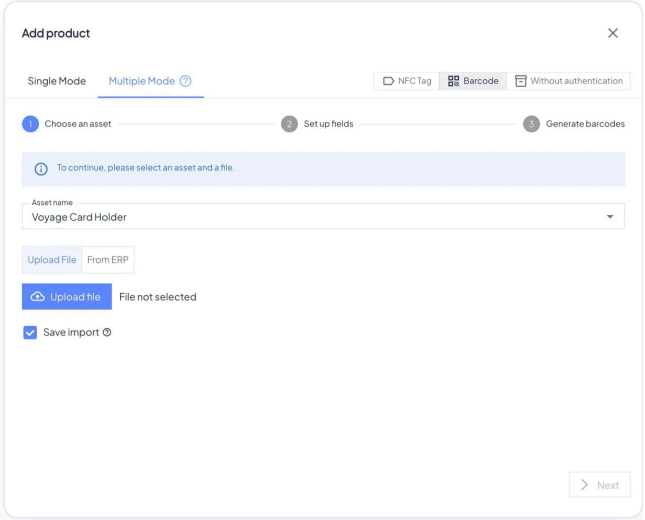
- **NFC Tag** : beschreibt den Tag auf dem Lesegerät. Der Administrationsbereich zeigt dessen Typ (NTAG 424, NTAG 215, EM4425).
- **Barcode** : erstellt ein Produkt mit QR-/Barcode-Authentifizierung; keine Hardware erforderlich.
- **Without authentication** : erstellt nur das Produkt; Tag oder Code können später auf seiner Seite ergänzt werden.

Einzelmodus

Asset wählen → Tag auflegen / Werte eingeben → Schreiben. Wählen Sie das Asset unter **Asset name** , füllen Sie die Felder aus und klicken Sie auf **Write** (oder **Create**). Nach dem Schreiben öffnet sich die Produktseite.



Barcode, Single mode: die auszufüllenden Asset-Felder.



Multiple mode: viele Produkte aus einer Datei, einer Anzahl oder einem ERP erstellen.

Mehrfachmodus

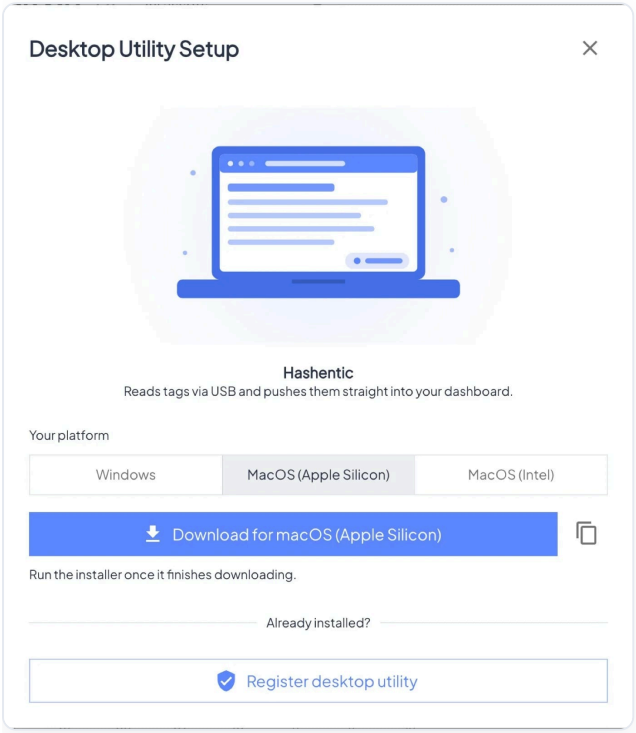
Asset wählen → Felder zuordnen → Tags beschreiben / Barcodes erzeugen.

- ✓ **Upload file**: CSV, XLSX oder XLS mit bis zu 100.000 Zeilen und 10 MB. Die erste Zeile enthält die Spaltennamen.
- ✓ **From ERP**: Datensätze aus einer gespeicherten ERP-Verbindung abrufen (Kapitel 17).
- ✓ Zeilen mit Validierungsfehlern sind markiert; korrigieren Sie diese vor dem Start über das Bearbeitungssymbol.

- **NFC-Tags** werden nacheinander beschrieben: Tag auflegen, auf "written" warten, entfernen, nächsten auflegen. Lassen Sie **Save import** aktiviert, um eine unterbrochene Sitzung fortzusetzen.
- **Generate by number**: nur eine Anzahl bis 50.000 für Assets ohne Pflichtfelder.
- **Set up fields** ordnet jedes Asset-Feld einer Spalte zu. Spalten mit exakt dem Eigenschaftsnamen eines Feldes werden automatisch zugeordnet.
- **Barcodes** werden im Hintergrund als Massenoperation erzeugt; Sie können die Seite schließen.
- Aktivieren Sie **Confirm on tag override**, um das Überschreiben eines bereits beschriebenen Tags bestätigen zu müssen.

Schreibvorgänge stoppen am monatlichen NFC-Tag- oder QR-Code-Limit Ihres Tarifs: Administrationsbereich, mobile App und Desktop-Dienstprogramm zeigen *Monthly NFC tag limit reached* oder *Monthly QR code limit reached* (siehe Monatslimits und Pakete).

Das Desktop-Dienstprogramm



Desktop Utility Setup, über das Menü (**Setup desktop utility**) oder **System → Applications**.

Das Desktop-Dienstprogramm ist eine kleine Anwendung für **Windows** und **macOS** (Apple Silicon und Intel), die ein USB-NFC-Lesegerät mit Ihrer Browsersitzung verbindet. Es läuft im Infobereich und bietet verfügbare Updates an.

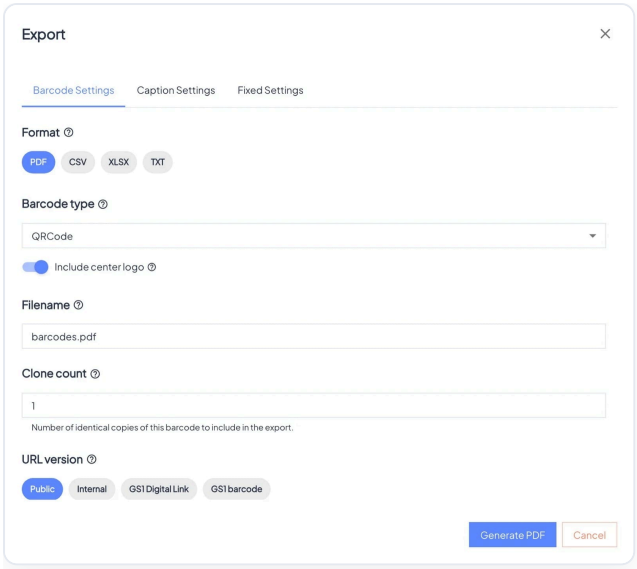
1. Laden Sie es aus dem Einrichtungsdialog herunter und installieren Sie es.
2. Klicken Sie auf **Register desktop utility**: Die App öffnet sich und meldet sich mit Ihrem Konto an. Alternativ fügen Sie den **Desktop application token** aus System → Applications ein.
3. Schließen Sie das Lesegerät an. Nach der Anmeldung wird die obere Schaltfläche grün: **Connected**; der Dialog Add product zeigt, ob auch das Lesegerät verbunden ist.

Das Dienstprogramm muss mit demselben Konto wie der Browser angemeldet sein. Die obere Schaltfläche zeigt *Connect frontend* (Browser nicht verbunden), *Connect application* (Dienstprogramm läuft nicht oder ist nicht angemeldet) oder *Connected*. Ein oranger Status bedeutet, dass das Lesegerät nicht mehr antwortet: Ziehen Sie es ab und schließen Sie es wieder an.

Barcodes exportieren

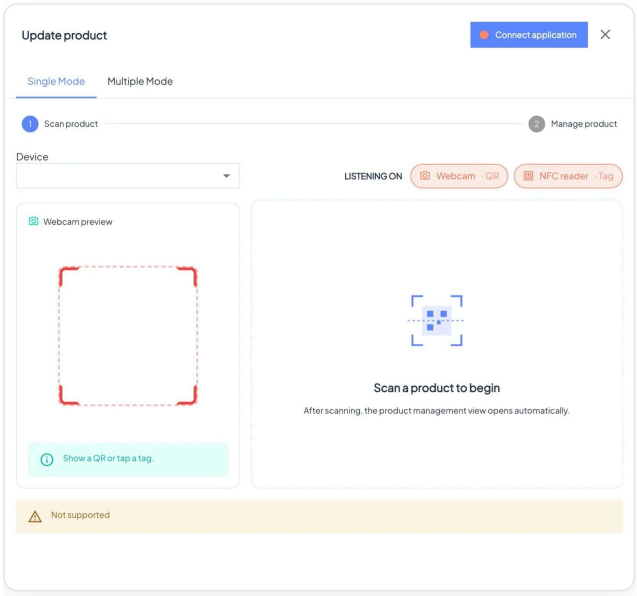
Öffnen Sie **Download** an einem Produkt, **Download barcodes** im Products-Tab eines Assets (exportiert alle Filtertreffer) oder an einer abgeschlossenen Massenoperation.

- **Format**: PDF (druckfertige A4-Bögen) oder Linklisten als CSV, XLSX, TXT.
- **Barcode type**: QR-Code, DataMatrix oder Code 128; optional mit Ihrem Logo in der Mitte des QR-Codes.
- **URL version**: *Public* (Ihre Verifizierungsadresse), *Internal* und bei GS1-Assets *GS1 Digital Link* und *GS1 barcode*.
- **Size**: fünf Vorgaben von Extra small bis Extra large oder eigene Maße mit Hinweisen zur Lesbarkeit.
- **Caption settings**: Feldwert oder eigenen Text unter jeden Code drucken.
- **Fixed settings**: Seiten, Codes pro Seite und Raster des resultierenden Bogens.



Export: Format, Codetyp, URL-Version und Größe.

Produkte aktualisieren



Update product: mit Webcam oder NFC-Lesegerät scannen.

Products → **Update** findet Produkte durch Scannen: Zeigen Sie den QR-Code Ihrer Webcam oder halten Sie den Tag an das Lesegerät.

- **Single mode** öffnet die gescannte Produktseite zur Bearbeitung.
- **Multiple mode** sammelt Produkte (durch Scannen, aus der Scanwarteschlange der mobilen App oder per Asset-Abfrage), erlaubt gemeinsame Werte mit individuellen Abweichungen und aktualisiert im Hintergrund.

Nur Felder der Stufe *Update* lassen sich nach dem Anlegen ändern. Die Bearbeitung benötigt die Lizenzfunktion Update records.

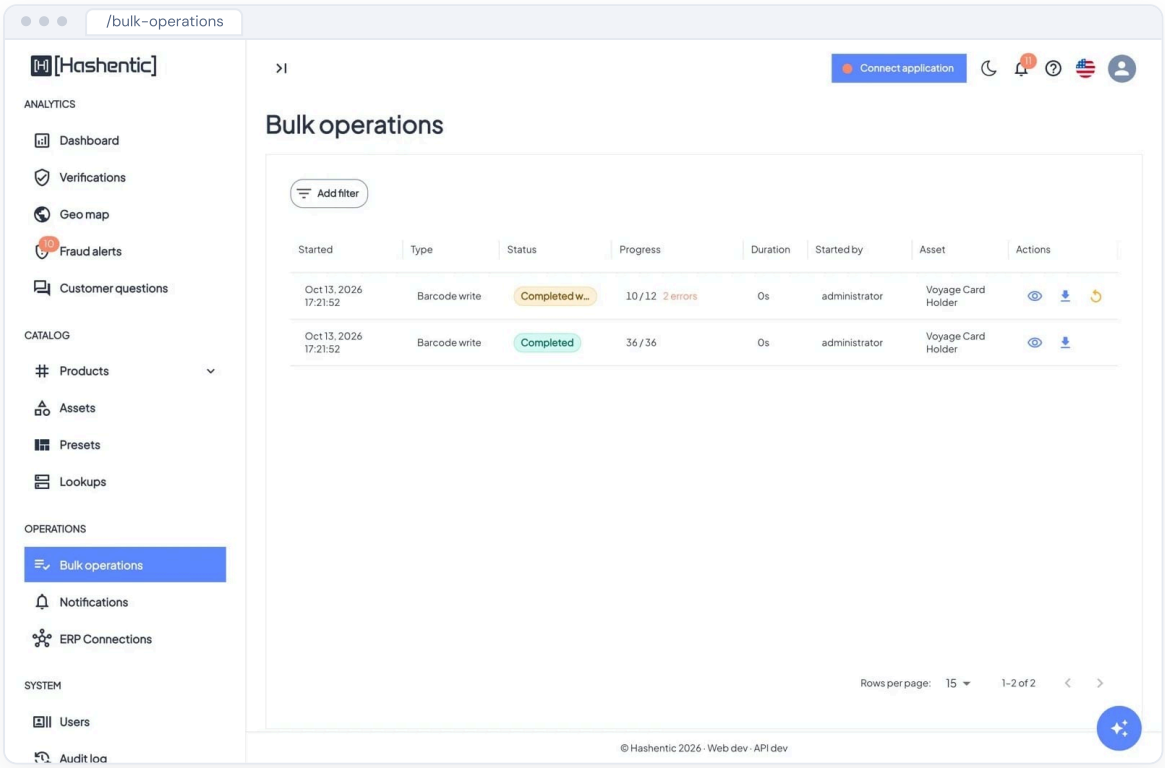
BETRIEB

17 Massenoperationen und ERP

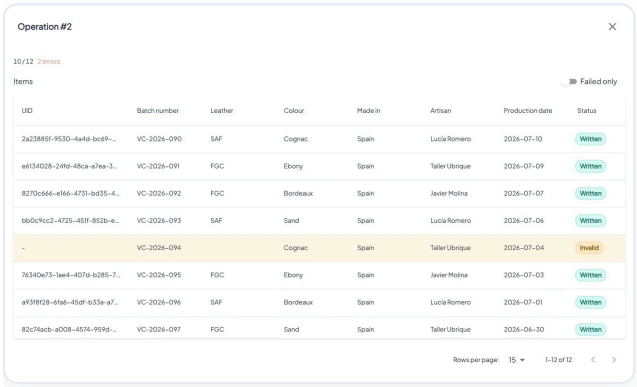
Große Aufgaben laufen im Hintergrund und werden hier verfolgt. ERP-Verbindungen bringen Produktdaten direkt aus Ihren Systemen in den Assistenten zum Beschreiben von Tags.

Massenoperationen

Menü Operations → Bulk operations **Berechtigung** Read / Write bulk operations **Lizenz** Bulk write



Massenoperationen: Barcode-Erzeugungen und Massenaktualisierungen mit Status, Fortschritt, Dauer und auslösender Person.



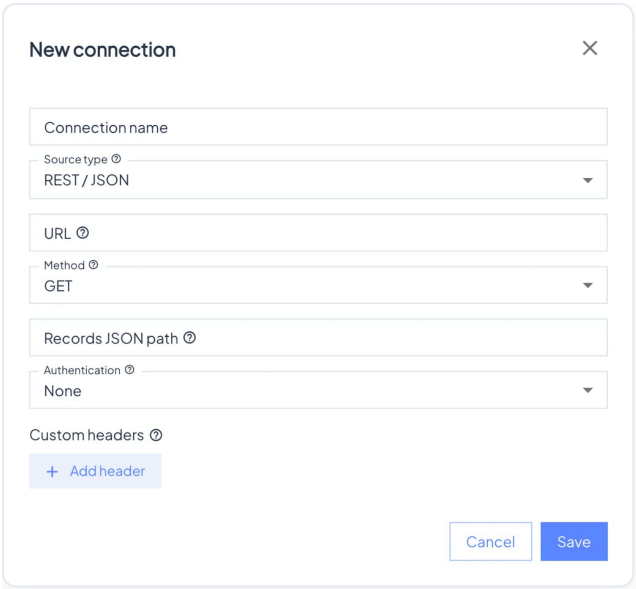
Vorgangsdetails: alle Einträge mit Status; **Failed only** zeigt den Korrekturbedarf.

- **Status**: Pending, Running, Completed, Completed with errors, Failed, Cancelled.
- **View details** listet die Einträge auf. Bearbeiten Sie eine fehlerhafte Zeile und wiederholen Sie sie oder nutzen Sie **Retry failed** für alle.
- **Download barcodes** exportiert die Codes eines abgeschlossenen Durchlaufs.
- **Cancel** beendet einen laufenden Vorgang; bereits erledigte Einträge bleiben erhalten.

ERP-Verbindungen

Menü Operations → ERP Connections **Berechtigung** Manage ERP connections **Lizenz** Bulk write

Speichern Sie eine wiederverwendbare, ausschließlich lesende Verbindung zu Ihrem ERP oder Ihrer Produktdatenbank:



Neue Verbindung zu einer REST-/JSON-Quelle.

- **REST / JSON**-, **JSON-RPC**- und **GraphQL**-APIs, ohne Authentifizierung, mit Bearer-Token, Basic-Authentifizierung oder API-Key-Header sowie eigenen Headern.
- **SQL-Datenbanken**: PostgreSQL, SQL Server, Oracle, MySQL/MariaDB mit einer einzelnen schreibgeschützten Abfrage.
- **MongoDB** mit Collection, Filter und Projektion.

Geheimnisse werden verschlüsselt gespeichert und maskiert angezeigt. Jede Verbindung gehört ihrer erstellenden Person. Nutzen Sie sie unter **Add new** → **Multiple mode** → **From ERP**: **Test / preview** zeigt die ersten 50 Datensätze, **Fetch records** lädt bis zu 100.000.

Aus Sicherheitsgründen werden Verbindungen zu lokalen oder privaten Netzwerkadressen abgelehnt.

BETRIEB · SYSTEM

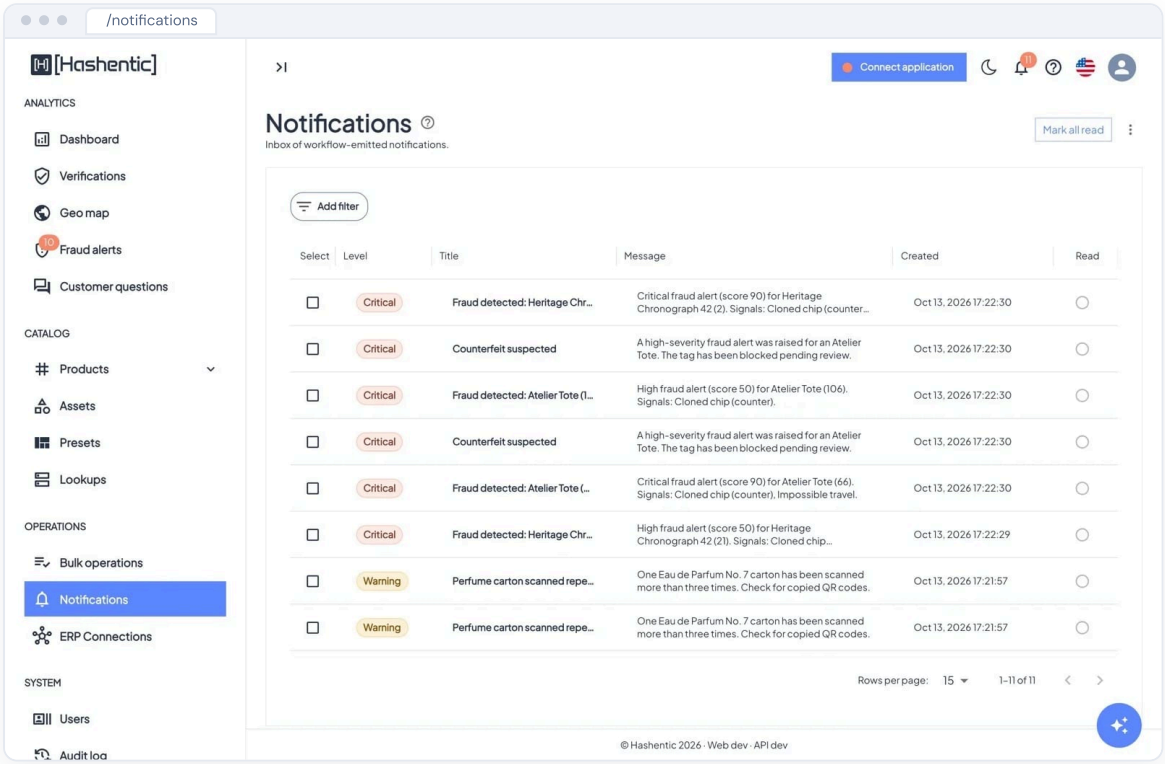
18 Benachrichtigungen und Audit-Protokoll

Benachrichtigungen zeigen Handlungsbedarf; das Audit-Protokoll dokumentiert, wer was getan hat.

Benachrichtigungen

Menü Operations → Notifications und die Glocke in der Kopfzeile

Berechtigung Read notifications



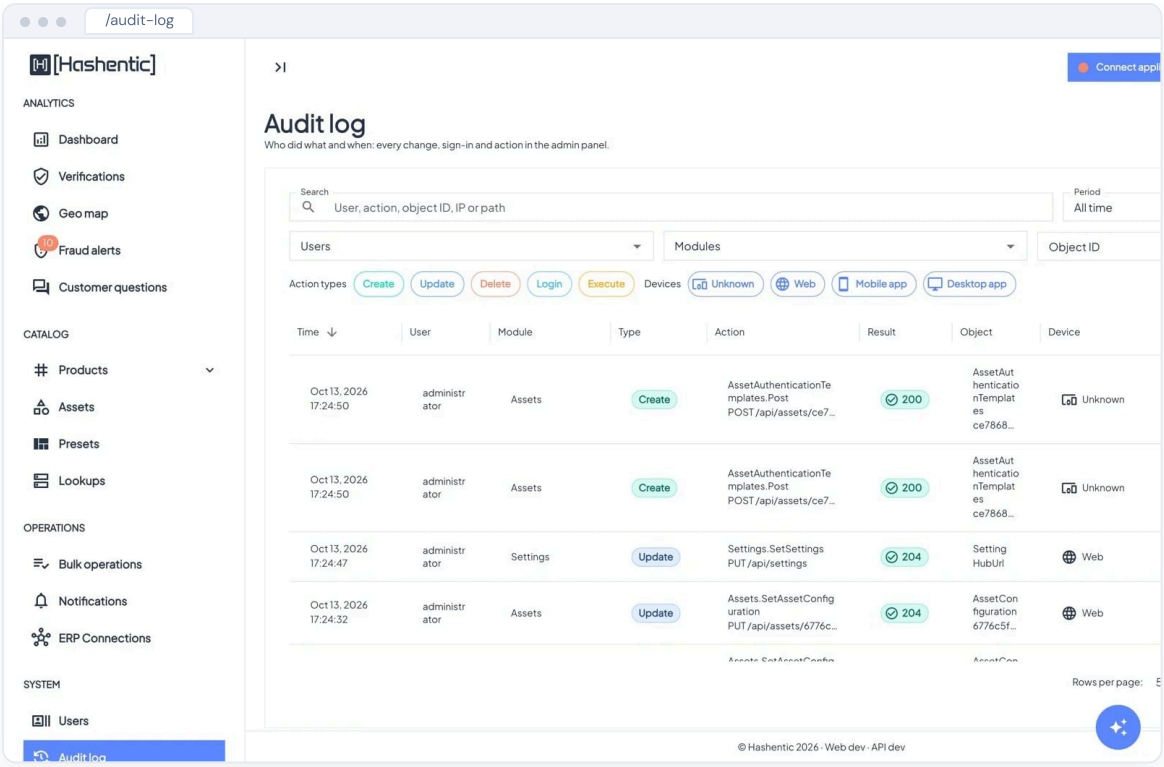
Benachrichtigungen der Betrugserkennung und aus Workflows nach Stufe: Info, Warning, Critical.

- Systembenachrichtigungen: *Fraud detected* (High- und Critical-Alarme), *Counterfeit anomaly* (gehäufte Fehlscans), *High verification count* und *License expires in N days*.
- Filtern Sie nach **Unread only** und Datum; markieren Sie als gelesen oder wählen Sie Einträge zum Löschen.
- Workflow-Benachrichtigungen mit eigenem Titel und Text.
- Öffnen Sie eine Benachrichtigung für Details, Produkt und den Workflow-Durchlauf, der sie versandt hat.

Audit-Protokoll

Menü System → Audit log

Zugriff Nur Super User



Audit-Protokoll: jede Änderung, Anmeldung und Aktion aus Web, mobiler App und Desktop-Dienstprogramm.

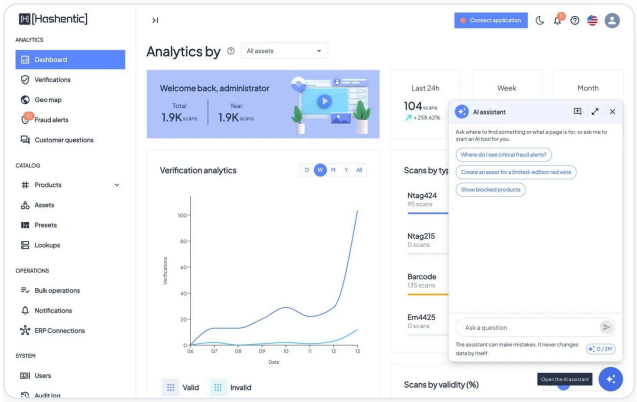
Filtern Sie nach Zeitraum, Benutzern, Modulen (Users, Settings, Assets, Products, Workflows, License, AI …), Aktionstyp (Create, Update, Delete, Login, Execute), Gerät und Ergebnis. Öffnen Sie einen Eintrag für genaue Änderungen (alte → neue Werte) und springen Sie zu **Show all activity of this user** oder **Show history of this object**.

19 KI-Funktionen

KI unterstützt an vier Stellen: Sie beantwortet Kundenfragen und Ihre Fragen, analysiert Scandaten und entwirft Konfigurationen. Daten ändert sie nie eigenständig.

Einstellungen KI-Analyse, KI-Assistent und Kundenantworten werden unter Settings aktiviert

Lizenz AI sowie AI assistant / AI analysis / Customer AI



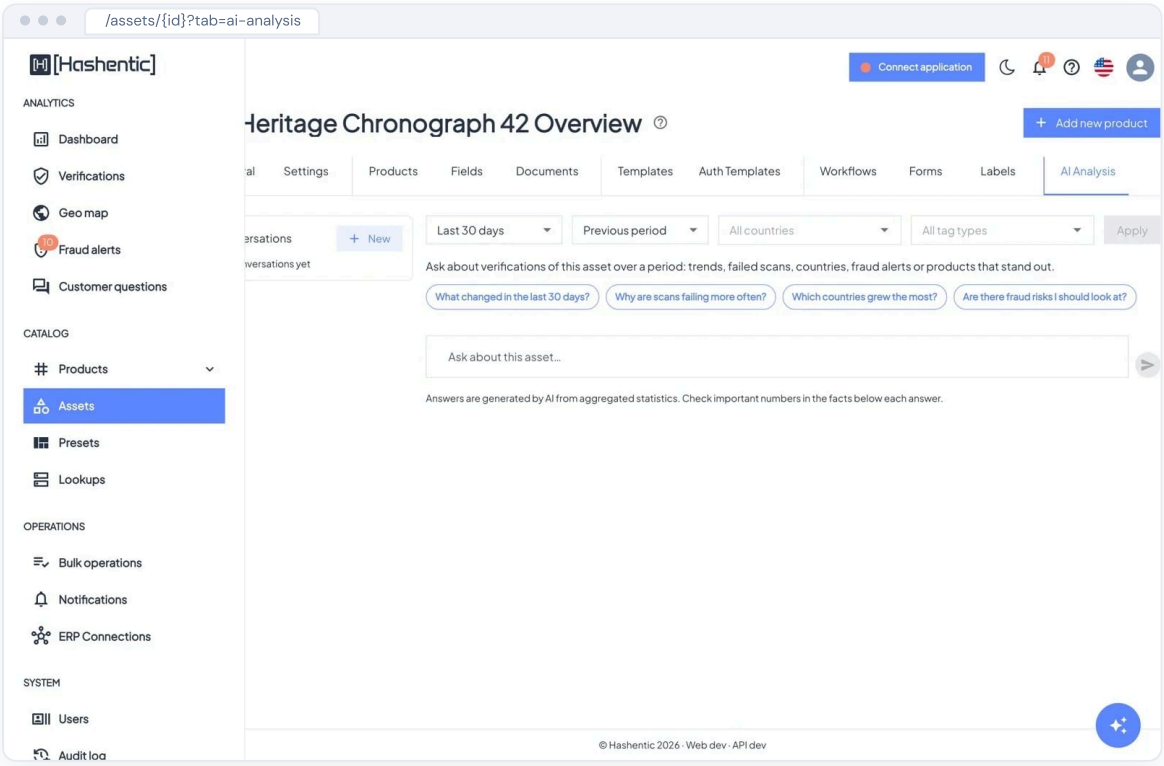
KI-Assistent, geöffnet über die Schaltfläche mit dem Funkensymbol.

KI-Assistent

Fragen Sie, wo sich etwas befindet oder wie eine Aufgabe erledigt wird: "Wo sehe ich kritische Betrugsalarme?", "Zeige gesperrte Produkte", "Erstelle einen Workflow, der mir Fehlscans per E-Mail meldet". Antworten enthalten Schaltflächen zur passenden Seite oder einem KI-Werkzeug. Auf einer Asset- oder Produktseite nutzt der Assistent auch die Dokumente dieser Linie.

KI-Analyse

Der Tab **AI analysis** an Assets und Produkten beantwortet Fragen zu Ihren Scans ("Warum schlagen Scans häufiger fehl?", "Welche Länder sind am stärksten gewachsen?") mit Erkenntnissen, Empfehlungen, einem Diagramm und den verwendeten Zahlen. An den KI-Dienst gehen nur aggregierte Anzahlen, Daten, Ländercodes, gerundete Standorte und Produktlabels; niemals IP-Adressen, Browserdetails, Formularantworten oder Eigentümerdaten.



KI-Analyse mit Filtern für Zeitraum, Vergleich, Land und Tag-Typ sowie vorgeschlagenen Fragen.

Antworten für Kunden

Der Assistent auf der Verifizierungsseite antwortet in der Kundensprache aus öffentlichen Feldern, Passdaten und öffentlichen Dokumenten. Siehe Kundenfragen.

Generatoren

Asset aus einer Beschreibung erstellen, Felder und Seitenvorlage erzeugen, Schutzempfehlungen erhalten, Kundenformulare gestalten und Workflows entwerfen oder ändern.

Dokumente: das Wissen der KI

Laden Sie Handbücher, Pflegehinweise, Garantiebedingungen und Zertifikate (PDF, DOCX, TXT oder Markdown) auf drei Ebenen hoch: **Settings** → **Brand documents** für die gesamte Marke, **Documents** am Asset für eine Produktlinie und **Documents** am Produkt für einen Artikel. Legen Sie für jedes Dokument **Audience** fest:

- ✓ **Internal only** (Standard): vom KI-Assistenten und der Analyse für Ihr Team verwendet.
- ✓ **Behörden, Recycler, Reparaturbetriebe**: für Partner des Digitalen Produktpasses.
- ✓ **Public**: von der Verifizierungsseite herunterladbar, für Kundenantworten genutzt und mit optionalem dauerhaftem öffentlichem Link.
- ✓ Jedes Dokument wird für KI indexiert; der Status *Indexed* zeigt seine Einsatzbereitschaft.

Damit Dokumente durchsuchbar werden, wird der Text jedes Dokuments, auch interner, an den auf dem Lizenzserver konfigurierten Embeddings-Anbieter gesendet. Für Kundenantworten werden nur öffentliche Dokumente verwendet. Laden Sie keine Dokumente mit personenbezogenen Daten hoch.

Welcher KI-Anbieter verwendet wird

Der KI-Anbieter wird auf dem Lizenzserver ausgewählt. Anbieter, die Daten außerhalb der EU ohne Angemessenheitsbeschluss verarbeiten (DeepSeek, GLM), werden nicht für Funktionen eingesetzt, die personenbezogene Daten enthalten können: Kundenfragen, Indexierung und Suche von Dokumenten, KI-Analyse, KI-Assistent und Workflow-Änderungen brechen mit einem Hinweis ab, einen anderen Anbieter zu wählen, während die Generatoren für Felder, Vorlagen, Formulare und Übersetzungen weiter funktionieren. Für OpenAI-Embeddings wird der EU-Endpunkt https://eu.api.openai.com/v1/embeddings empfohlen.

SYSTEM

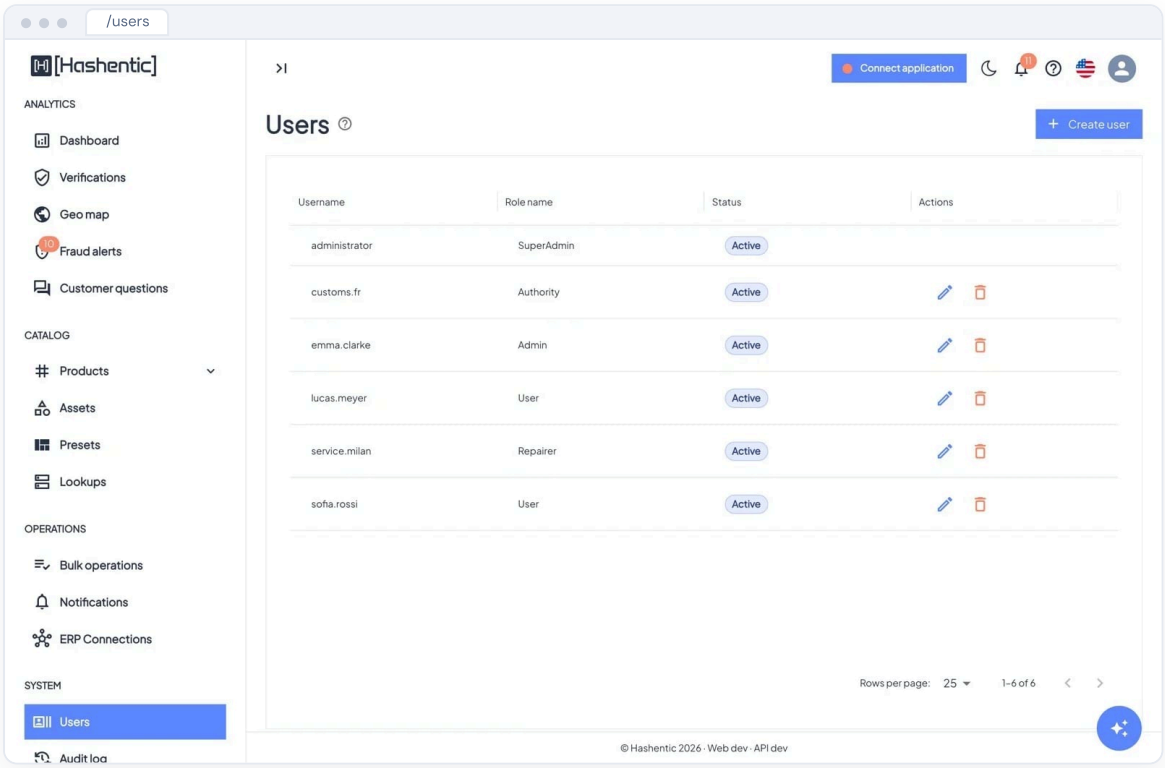
20 Benutzer und Zugriff

Geben Sie jeder Person ein eigenes Konto mit genau den Berechtigungen und Produktlinien, die ihre Aufgabe erfordert.

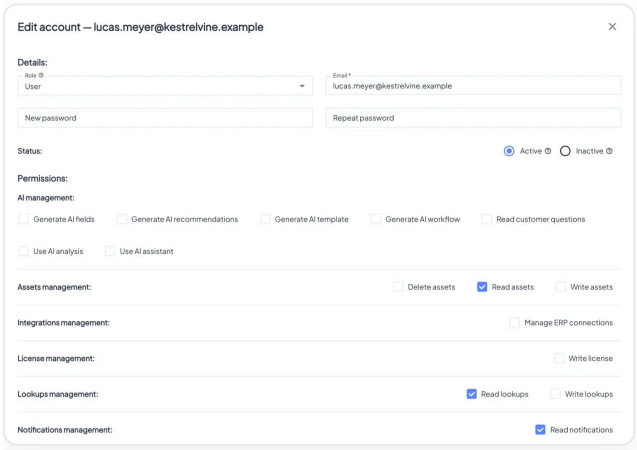
Menü System → Users

Berechtigung Read / Write users

Limit Benutzeranzahl Ihrer Lizenz



Benutzer mit Rolle und Status. Der Stift bearbeitet ein Konto, der Papierkorb löscht es.



Konto bearbeiten: Angaben, Status und Berechtigungen.

Create user fragt folgende Angaben ab:

- **Username** und **Email**.
- **Role**: Admin, User oder eine Partnerrolle (Authority, Recycler, Repairer). Zur Rolle gehörende Berechtigungen sind aktiviert und können nicht entfernt werden.
- **Password**: mindestens 12 Zeichen mit einem Buchstaben und einer Ziffer. Sie legen es fest und geben es weiter; es wird keine Einladungs-E-Mail versandt.
- **Status**: Active-Benutzer können sich anmelden; Inactive-Benutzer behalten ihre Daten, können sich jedoch nicht anmelden.
- **Permissions**, nach Bereichen gruppiert.
- **Allowed assets** für Rollen, die nicht alles sehen.

Um ein Passwort zurückzusetzen, geben Sie beim Bearbeiten des Kontos ein neues ein; dadurch wird die Person auch abgemeldet. Niemand kann eine höhere Rolle oder Berechtigungen vergeben, die er selbst nicht besitzt.

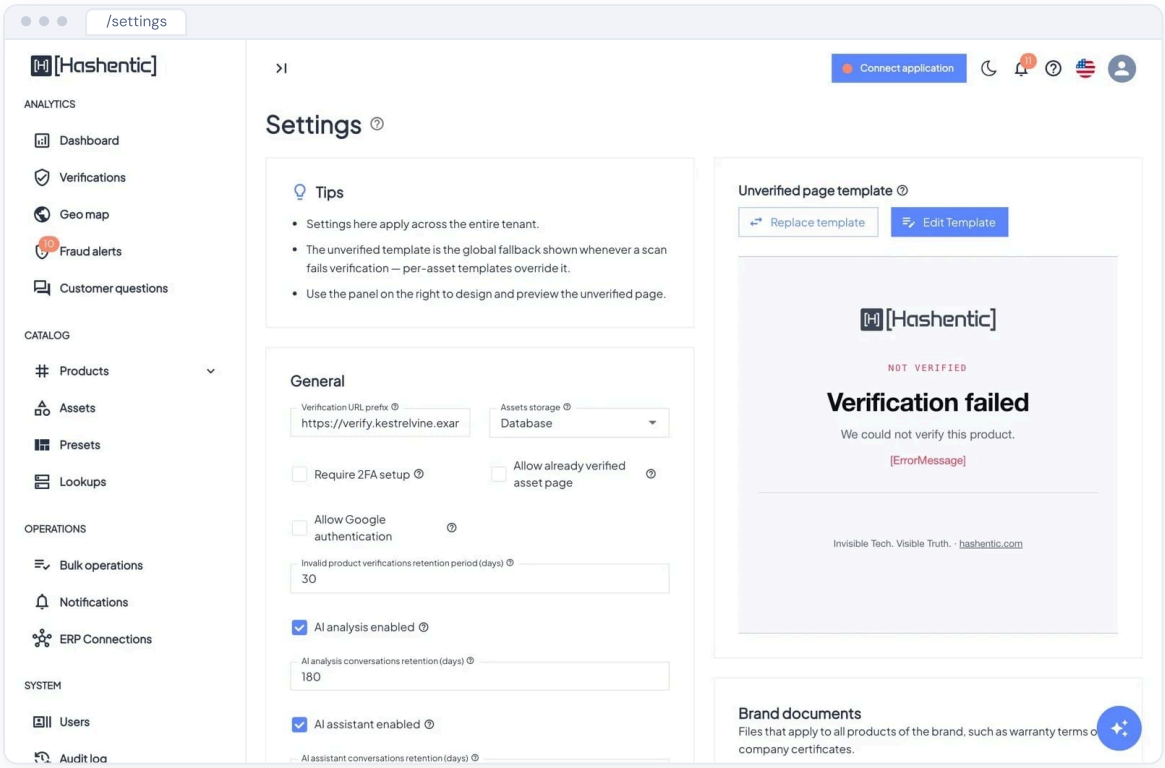
SYSTEM

21 Einstellungen, Branding und Lizenz

Konfiguration für den gesamten Arbeitsbereich: Verifizierungslinks, Sicherheitsregeln, KI-Schalter, Empfindlichkeit der Betrugserkennung, Markenauftritt und Lizenz.

Einstellungen

Menü System → Settings **Berechtigung** Read / Write settings



Einstellungen. Allgemeine Einstellungen links; globale Seite für ungültige Scans, Markendokumente und URL-Freigabeliste für Workflows rechts.

Einstellung	Wirkung
Verification URL prefix	Öffentliche Adresse am Anfang jedes Verifizierungslinks und QR-Codes, etwa `https://verify.your-brand.com/v` . Muss https verwenden.
Default NTAG 424 key	Schlüssel für neue NTAG-424-Tags. Änderungen wirken sich nur auf anschließend beschriebene Tags aus.
Assets storage	Speicherort der Integritätsnachweise: Database oder Blockchain. Nur lesbar: wird einmalig bei der Installation gewählt und kann hier nicht geändert werden. Hub-URL und Link zum Blockchain-Explorer können aus der Serverumgebung kommen; ein hier gespeicherter Wert hat Vorrang, etwa nach einem Domainwechsel.
Require 2FA setup	Jeder Benutzer muss bei der Anmeldung Zwei-Faktor-Authentifizierung einrichten und kann sie nicht deaktivieren.
Allow Google authentication	Bestehende Benutzer können sich mit dem Google-Konto anmelden, das ihrer E-Mail-Adresse entspricht.
Allow already verified asset page	Gestaltete Produktseite bei wiederholten Scans sicherer Tags anzeigen. Aktiviert gilt dies für jedes Asset; deaktiviert kann jedes Asset es weiterhin selbst aktivieren.

Einstellung	Wirkung
AI analysis / AI assistant enabled · Answer customer questions on the verification page	Aktiviert KI-Funktionen mit Aufbewahrungszeiträumen und Tageslimit für Kundenfragen.
Maximum document file size (MB)	Uploadlimit für Dokumente, 1–25 MB (Standard 10).
Invalid product verifications retention period (days)	Aufbewahrungsdauer fehlgeschlagener Scans (Standard 30).
Scan IP address retention (days)	Nach dieser Anzahl Tage (Standard 365, bis 3650) behalten Scans und fehlgeschlagene Scans nur eine gekürzte IP-Adresse (IPv4 /24, IPv6 /48). Standort, Land, Gerät und der Scan selbst bleiben erhalten, Karte und Analysen bleiben also unverändert.
Verification alerts	Critical-Benachrichtigung, wenn ein Produkt in einer Stunde mehr Fehlscans als den Schwellenwert erreicht (Standard 5), und Warning bei einer Scananzahl eines Tags (Standard 1.000).
Fraud & anomaly detection	Ein/Aus und alle Schwellen der Betrugserkennung: Reisegeschwindigkeit und Entfernung, Scanratenzeitraum und Anzahl, Graumarktscans und Zeitraum, Fehlscan-Häufungszeitraum, Alarmruhezeit, High- und Critical-Wertgrenzen.

Rechts gestalten Sie außerdem die **Unverified page template** (für fehlgeschlagene Scans von Assets ohne eigene Vorlage) mit Sprachen, ergänzen **Failed page rules** zur Auswahl anderer Fehlerseiten für alle Produkte nach Fehlergrund, Tag-Typ oder Land (Verifizierungsseitenvorlagen), verwalten **Brand documents** für KI-Antworten und pflegen die **Workflows URL allowlist** der erlaubten Zieladressen.

Von Blockchain- zu Datenbankspeicherung wechseln

Bei einer Installation, die Integritätsnachweise auf der Blockchain speichert, kopiert die Karte **Move to database storage** rechts den gesamten Verlauf in die Datenbank und stellt die Installation anschließend um. Dafür ist **Write settings** erforderlich.

1. Klicken Sie auf **Copy history**. Die Kopie läuft im Hintergrund und ändert nichts für die Benutzer; die Karte zeigt Fortschritt und Probleme. Wiederholen Sie den Vorgang, bis keine Probleme mehr aufgeführt sind.
2. Sichern Sie die Datenbank.
3. Klicken Sie zu einer ruhigen Zeit auf **Switch to database** und bestätigen Sie. Der Verlauf wird noch einmal kopiert, die Installation schreibt ab dann in die Datenbank, eine abschließende Prüfung bestätigt, dass nichts fehlt, und als Speicher wird Database gespeichert.

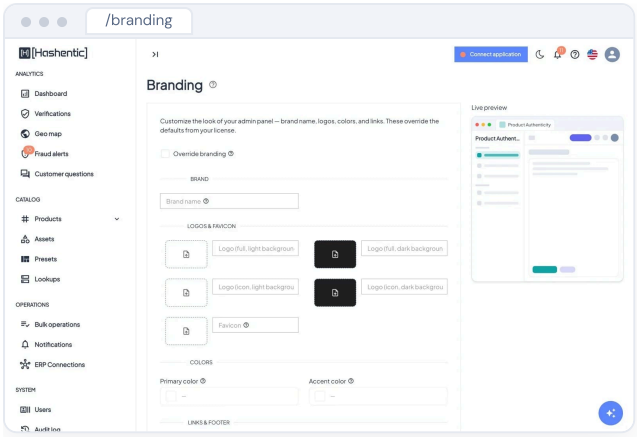
Der Wechsel geht nur in eine Richtung: Im Administrationsbereich gibt es keinen Weg zurück zur Blockchain, und die Dienste starten nicht, wenn der Server bei einer Datenbankinstallation `ASSETS_STORAGE=Blockchain` setzt. Solange der Server `ASSETS_STORAGE=Blockchain` setzt, bleibt **Switch to database** deaktiviert. Der Wechsel startet nicht, solange Massenoperationen oder Workflows laufen oder Blockchain-Transaktionen noch ausstehen; die Karte listet auf, was zu beheben ist. Wurde der Wechsel unterbrochen, schließt **Finish the switch** ihn ab. Nach dem Wechsel werden keine Blockchain-Explorer-Links mehr angezeigt.

Branding

Menü System → Branding **Lizenz** White-label branding

Aktivieren Sie **Override branding**, um die Lizenzvorgaben durch eigene Angaben zu ersetzen:

- **Brand name** für Administrationsbereich, Seitentitel und Verifizierungsseiten.
- **Logos** (vollständig und als Symbol, für helle und dunkle Hintergründe) und **Favicon**. Das Symbollogo wird auch in QR-Codes eingebettet.
- **Primär- und Akzentfarben**.

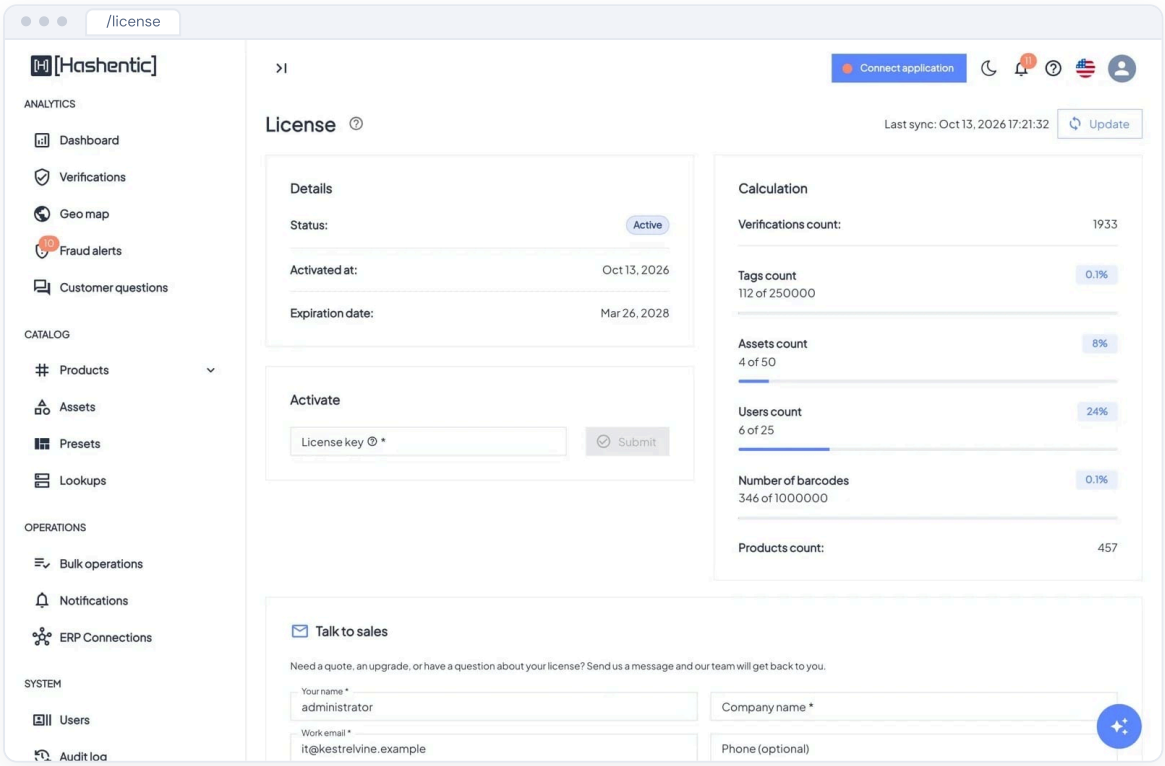


Branding mit Live-Vorschau rechts.

- **Links**: Website, Support, Datenschutz, Bedingungen; **Fußzeile** und **"Powered by"**-Text auf Verifizierungsseiten. Ohne URL zur Datenschutzerklärung zeigt die Verifizierungsseite einen integrierten Datenschutzhinweis.

Lizenz

Menü System → License **Berechtigung** Write license



Lizenz. Status und Daten, Nutzung gegenüber Limits, Aktivierung und Kontaktformular.

- **Details**: Status (Active, Expired, Blocked, Stale, Inactive), Aktivierungs- und Ablaufdatum.
- **Activate**: Lizenzschlüssel einfügen (Format XXXX-XXXX-XXXX-XXXX-XXXX). Aktivierungslinks aus E-Mails werden nach der Anmeldung automatisch angewandt.
- **Calculation**: Verifizierungen, Tags, Assets, Benutzer, Barcodes und Produkte mit Fortschrittsbalken gegenüber Ihren Limits.
- **Tarif**: Der Chip neben dem Seitentitel nennt Ihren Tarif: Free, Start, Pro, Business, Enterprise, Trial oder Individual (ein mit Ihnen vereinbarter Tarif).
- **This month** : **Scan analytics** , geschriebene QR-Codes, geschriebene NFC-Tags und Workflow-Durchläufe dieses Monats gegenüber Ihrem Monatslimit, dazu die gemessenen Dienste (E-Mails, Geolokalisierungsabfragen, KI-Tokens, Produktabfragen, KI-Antworten für Kunden). Die Limits enthalten gekaufte Prepaid-Pakete (*incl. N from packs*). Die Zähler werden am 1. jedes Monats (UTC) zurückgesetzt.

- **Purchased packs**: jedes Prepaid-Paket mit Menge, Kaufdatum, letztem gültigen Tag (ein UTC-Datum, in jeder Zeitzone gleich), verbrauchter und verbleibender Menge und Status (Active, Used up, Expired, Voided) sowie dem Rest je Art. Lange Verläufe zeigen 25 Pakete auf einmal (**Show more**). Pakete fügt Ihr Account-Manager hinzu; ohne Pakete sehen Sie *No packs yet — contact your account manager to top up*. Bietet Ihr Tarif keine Pakete an (bei Free und während der Testphase immer), zeigt die Karte stattdessen *Your plan does not include packs*; haben Sie noch Pakete aus einem früheren Tarif, listet sie sie unter *Your current plan does not offer packs* auf, und sie zählen weiter, bis sie aufgebraucht sind oder ablaufen. Wenn Ihr Tarif Pakete verkauft, können Sie über **Order a pack** auf dieser Karte selbst eines bestellen (siehe Paket bestellen); Ihre Bestellungen stehen unter **Pack orders** mit dem Status *Awaiting payment*, *Paid, pack added* oder *Cancelled*, und eine leere Karte zeigt dann *No packs yet. Order a pack to top up your monthly limits.*
- **Update** ruft den neuesten Lizenzstand ab; **Talk to sales** sendet eine Nachricht an das Hashentic-Team.

Monatslimits und Pakete

Jeder Tarif hat feste Monatslimits; eine automatische Abrechnung von Mehrverbrauch gibt es nicht. Brauchen Sie in diesem Monat mehr, kaufen Sie ein Prepaid-Paket oder wechseln Sie zu einem höheren Tarif (über **Talk to sales**). Ein neues Konto kann mit einer Testphase beginnen: einem Tarif mit kleinen Monatslimits für eine festgelegte Anzahl von Tagen (30, sofern Hashentic das nicht geändert hat). Das Ablaufdatum auf der Lizenzkarte zeigt, wann Ihre Testphase endet; danach wechselt Ihr Konto in den Tarif Free. Erreicht ein kostenpflichtiger Tarif (Start, Pro, Business oder Enterprise) sein Enddatum ohne Zahlung, wechselt das Konto zum Free-Tarif: Bereits ausgegebene Codes lassen sich weiter prüfen und gekaufte Pakete bleiben nutzbar; ein individueller Vertrag (Custom) endet wie vereinbart.

Was jeder Tarif enthält, etwa Monatslimits, Module und die angebotenen Pakete, legt Hashentic fest, und es kann sich ändern; die aktuellen Tarife finden Sie unter hashentic.com/license. Eine Änderung gilt nur, wenn einer Lizenz ein Tarif zugewiesen wird, etwa bei der Registrierung, am Ende der Testphase oder beim Wechsel in einen anderen Tarif. Ihre bestehende Lizenz behält ihre Limits und Module, und Ihre Lizenzkarte zeigt sie immer an.

Welche Pakete Sie kaufen können, hängt ebenfalls von den aktuellen Einstellungen Ihres Tarifs ab: Free und die Testphase bieten keine an, und die Karte **Purchased packs** zeigt an, wenn Ihr Tarif keine anbietet. Ein gekauftes Paket zählt weiter, bis es aufgebraucht ist oder abläuft, auch nachdem Sie in einen Tarif gewechselt sind, der diese Paketart nicht anbietet.

- **QR-Codes, NFC-Tags, Workflow-Durchläufe und gemessene Dienste** stoppen an ihrem Limit. Wenn Ihr Tarif ein Paket dieser Art anbietet, zeigt die Karte *Limit reached. Buy a pack or move to a higher plan.*; sonst (bei Free, während der Testphase, in einem Tarif ohne Paket dieser Art sowie bei E-Mails, Geolokalisierungen und Produktabfragen, für die es keine Pakete gibt) zeigt sie *Limit reached. Your plan has no pack for this, so move to a higher plan or wait for the monthly reset.* Schreibbildschirme zeigen *Monthly QR code limit reached* oder *Monthly NFC tag limit reached* mit demselben Hinweis. Das erneute Beschreiben eines bereits beschriebenen Tags zählt nicht noch einmal.
- **Scans sind unbegrenzt und werden nie blockiert.** Die Zeile **Scan analytics** zählt die Scans, die Standort- und Geräteanalysen erhalten. Oberhalb dieser Menge zeigt die Karte *Quota exceeded — buy a pack or upgrade* (in einem Tarif ohne Pakete: *Quota exceeded — move to a higher plan*); Scans funktionieren weiter, aber Standort- und Geräteanalysen pausieren, bis der Monat endet, Sie ein Paket kaufen oder in einen höheren Tarif wechseln.
- Ist der Lizenzserver nicht erreichbar, steht im Bereich der Dienste *Service usage is unavailable right now*, statt null anzuzeigen.

Paket bestellen

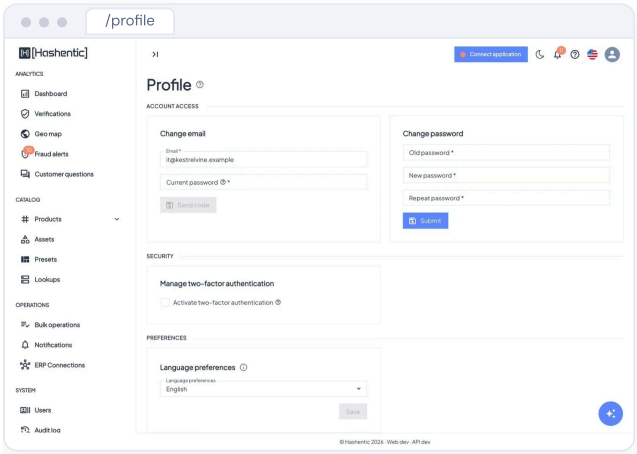
Ein Administrator mit der Berechtigung **Write license** kann auf der Lizenzseite ein Prepaid-Paket bestellen. Die Schaltfläche **Order a pack** erscheint nur, wenn Ihr Tarif Pakete verkauft: nicht auf Free, nicht in der Testphase, nicht bei einer abgelaufenen, gesperrten oder inaktiven Lizenz und nicht für Shops mit Abrechnung über Shopify, die Pakete in der Shopify-App kaufen.

1. Öffnen Sie System → License und klicken Sie auf der Karte **Purchased packs** auf **Order a pack**.
2. Wählen Sie **Pack** und **Size**. Jede Größe zeigt ihren Preis in Euro aus der aktuellen Hashentic-Preisliste; die Preise verstehen sich zzgl. MwSt.
3. Fügen Sie bei Bedarf eine **Note for our sales team (optional)** hinzu, zum Beispiel Ihre Bestellnummer (bis zu 500 Zeichen).
4. Klicken Sie auf **Place order**.

Hashentic sendet eine Rechnung an die E-Mail-Adresse der Lizenz; bezahlen Sie sie per Banküberweisung. Bis zum Zahlungseingang wartet die Bestellung als *Awaiting payment*. Danach fügt das Vertriebsteam das Paket hinzu und die Bestellung wechselt zu *Paid, pack added*. Das Paket erscheint in der Liste und zählt zu den Limits dieses Monats, sobald Ihre Lizenz aktualisiert wird (**Update** holt sie sofort). Das Paket gilt ab diesem Tag 12 Monate. Eine nicht bezahlte Bestellung kann das Vertriebsteam stornieren; sie zeigt dann *Cancelled*.

Es können höchstens 5 Bestellungen gleichzeitig auf Zahlung warten. Zeigt das Formular *Ordering packs is not available on this server yet*, muss Ihre Hashentic-Installation oder der Lizenzserver aktualisiert werden; bis dahin erhalten Sie Pakete über Ihren Account Manager.

Ihr Profil



Profil, über den Avatar in der Kopfzeile erreichbar.

- **Account access**: E-Mail-Adresse (Bestätigung durch Code an die neue Adresse) und Passwort ändern.
- **Security**: **Activate two-factor authentication** mit einer beliebigen Authenticator-App und Verwaltung Ihrer 10 einmaligen Wiederherstellungscodes.
- **Preferences**: Ihre Sprache für Administrationsbereich und E-Mails.

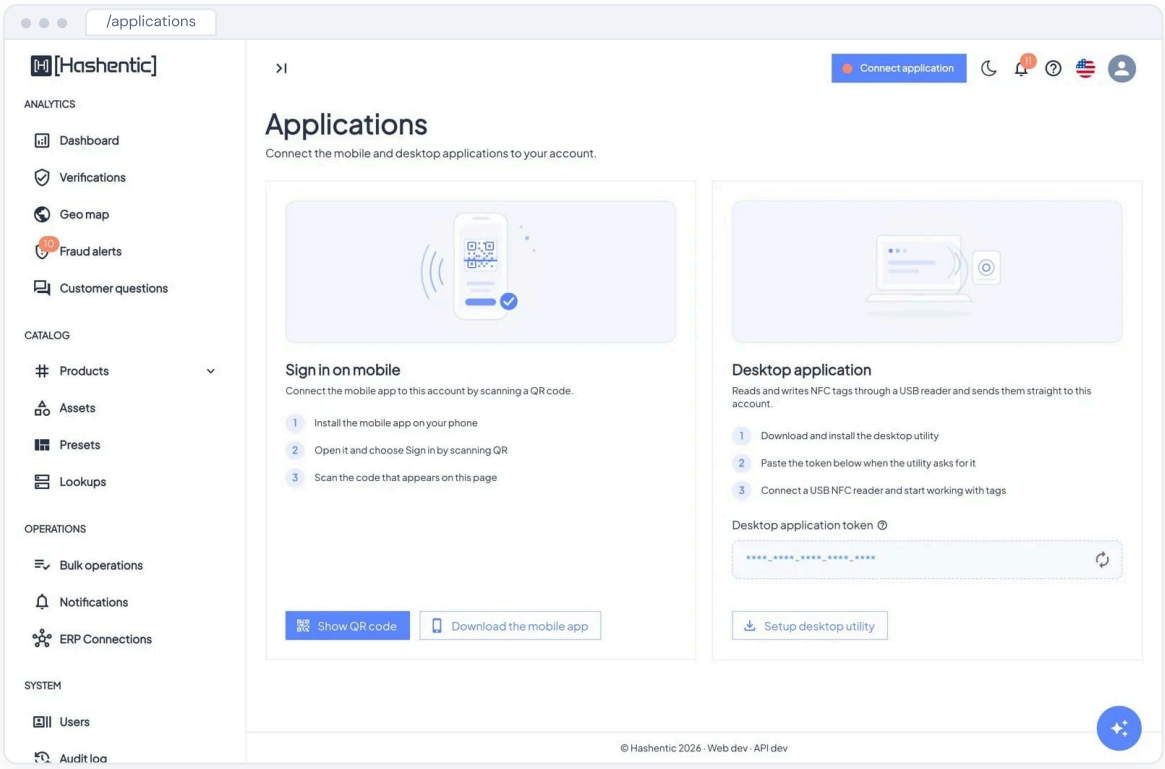
ANWENDUNGEN

22 Mobile App und Desktop-Dienstprogramm

Zwei Begleitanwendungen bringen Hashentic über den Schreibtisch hinaus: die mobile App für Mitarbeiter in Filialen, Lagern und Servicezentren sowie das Desktop-Dienstprogramm zum Beschreiben von NFC-Tags in der Produktion.

Menü System → Applications

Lizenz Mobile applications für die mobile App



Anwendungen. Per QR-Code mobil anmelden, Apps herunterladen und den Desktop application token abrufen.

Die mobile App

Verfügbar für **Android** ab 8.0 und **iPhone** ab iOS 16.4. Zum Lesen und Beschreiben von Tags benötigt Ihr Telefon NFC. Die App folgt der Telefonsprache (Englisch, Französisch, Portugiesisch oder Russisch) und unterstützt helle und dunkle Darstellung.

Für alle

- **Ist es echt?** Jeder kann ein Produkt ohne Konto prüfen: QR-Code scannen, **Read NFC tag** antippen oder den Link eingeben. Vor dem Öffnen der Markenseite prüft die App, ob der Link zu einem registrierten Hashentic-Arbeitsbereich gehört. Liest die Kamera einen Code, mit dem die App nichts anfangen kann, erscheint der Grund über dem Kamerabild, und das Scannen pausiert, bis Sie **Scan another code** antippen. Lässt sich die Markenseite nicht öffnen oder erreicht eine Prüfung den Server nicht, bietet die Fehlermeldung bei einem gedruckten Code (QR-Code, Barcode, Produktkennung) oder einem NTAG-215-Link **Retry** an, dazu **Scan another code** und **Back**. Ein sicherer Tag (NTAG 424, EM4425) erzeugt bei jedem Antippen einen neuen Link; statt **Retry** bittet die App deshalb, den Tag erneut anzutippen: Sie sendet einen Tag-Link nie ein zweites Mal und wiederholt keine Prüfung von sich aus.
- **Datenweitergabe**: Beim ersten Start zeigt die App den Bildschirm **Data sharing** mit einem Schalter für jede optionale Funktion, die Daten an einen Drittanbieterdienst sendet, zum Beispiel den KI-Assistenten auf Produktseiten, dessen Fragen an OpenAI gesendet werden, um eine Antwort zu erzeugen. Alle Schalter sind anfangs aus, keiner ist Pflicht: Tippen Sie mit allen Schaltern aus auf **Continue**, und die App funktioniert wie gewohnt. Ist der KI-Assistent ausgeschaltet, öffnen sich Produktseiten ohne den Assistenten. Der Bildschirm erscheint nur wieder, wenn sich die Liste ändert, und Ihre bisherige Wahl ist dann schon eingestellt. Ändern können Sie sie jederzeit unter **Settings** → **Data sharing**. Auf der Website gibt es keinen zusätzlichen Schritt.
- **Datenschutzerklärung**: **Privacy policy** unten auf dem Startbildschirm und unter **Settings** → **About the app** öffnet die Datenschutzerklärung in der Sprache der App.
- **Unternehmen und Kontakt**: **Settings** → **About the app** listet außerdem **Website**, **Legal notice** und **Support** (öffnet Ihre Mail-App), darunter den Firmennamen. Eine gebrandete App zeigt nur die Links, die ihre Marke bereitstellt.
- **Lizenzen von Drittanbietern**: **Settings** → **About the app** → **Third-party licenses** listet die Open-Source-Pakete der App; tippen Sie auf ein Paket, um seine Lizenz zu lesen.

Für Mitarbeiter

- **Anmelden** mit Arbeitsbereichsadresse, Benutzername und Passwort oder durch Scannen des QR-Codes aus **Applications** → **Sign in on mobile**. Zwei-Faktor-Authentifizierung und mehrere Konten werden unterstützt. Der Code-Bildschirm sagt, ob der sechsstellige Code aus der Authenticator-App oder einer der gespeicherten Wiederherstellungscodes einzugeben ist. **Sign out** unter **Settings** oder im Profil fragt vorher nach und nennt das Konto; bei mehreren Konten sagt die App auch, zu welchem sie wechselt.
- **Produkte**: nach Kennung oder Tag-UID suchen, nach Asset, Label, Tag-Typ und Status filtern und die Produktkarte mit Tags, Feldern und Verlauf öffnen.
- Produkte **anlegen** und Felder **bearbeiten** (bei sicheren Tags kann vorheriges Einlesen nötig sein).
- **NFC-Tags beschreiben** (NTAG 424, NTAG 215, EM4425) direkt per Telefon mit kryptografischem Rücklesen. Unterbrochene Schreibvorgänge können später abgeschlossen oder verworfen werden.
- **Pack order** für Shopify-Bestellungen mit NFC-Produkten: Scannen Sie den Packcode, den die Hashentic-App in Shopify bei der Bestellung anzeigt, oder geben Sie die Bestellnummer ein, und beschreiben Sie dann für jeden Artikel ein leeres Tag. Der Schreibbildschirm nennt Bestellung und Artikel; nach einem erfolgreichen Schreibvorgang bietet er statt eines weiteren Schreibvorgangs **Back to order** an, sodass jeder Artikel genau ein Tag erhält. Ein Artikel, der nach dem Beschreiben seines Tags aus der Bestellung entfernt wurde, ist als *removed from the order · tag written, do not ship* markiert: Nehmen Sie ihn aus dem Paket. Scannen Sie den Code einer anderen Bestellung, während noch Artikel warten, fragt die App vor dem Wechsel nach. Packcodes öffnen sich nur über den Scanner der App, nicht über Links. Pack order erscheint, wenn Ihr Arbeitsbereich mit Shopify verbunden ist, Sie die Berechtigung zum Schreiben von Produkten haben und die Lizenz **Mobile applications** sowie mindestens einen NFC-Tag-Typ umfasst.
- Produkte entsprechend Ihren Berechtigungen **sperren, entsperren oder löschen**. **Block** fragt vorher nach, denn die Tags des Produkts bestehen die Prüfung erst nach dem Entsperren wieder.
- **Produkt aus dem Web öffnen**: den **QR for the mobile app** auf einer Produktseite scannen.
- Partnerrollen (Behörde, Recyclingbetrieb, Reparaturbetrieb) sehen und bearbeiten nur die für sie bestimmten Passfelder.

- **App-Sperre** mit sechsstelliger PIN und/oder Face ID oder Fingerabdruck.
- **Produkt scannen** für ein grünes Ergebnis *Verified* oder rotes *Verification failed* mit Grund und öffentlichen Feldern. Das Ergebnis nennt auch den geprüften Tag-Typ (Barcode, NTAG424, NTAG215 oder EM4425). Anschließend Produkt öffnen oder **Save for batch update** wählen.

Das Desktop-Dienstprogramm

Eine kleine Windows- und macOS-App verbindet ein USB-NFC-Lesegerät mit Ihrem Konto; Sie arbeiten weiter im Browser. Die App folgt der Systemsprache: Deutsch, Englisch, Spanisch, Französisch, Polnisch, Portugiesisch, Russisch oder Chinesisch; bei anderen Sprachen erscheint sie auf Englisch. Laden Sie sie unter **Setup desktop utility** herunter, melden Sie sich mit **Register desktop utility** oder dem **Desktop application token** an und schließen Sie das Lesegerät an. Führt ein Anmeldelink zu einem anderen Server als dem verbundenen oder ist es die erste Anmeldung per Link, nennt die App den Server und fragt vorher: **Anmelden** verbindet, **Abbrechen** lässt alles unverändert. Fahren Sie nur fort, wenn Sie den Link selbst geöffnet haben. Werden in diesem Moment Tags geschrieben, fragt die App noch einmal: **Server wechseln nach Abschluss** wechselt, sobald sie fertig sind, **Abbrechen** bleibt verbunden. Ein Link schließt die laufende App nie. Sie läuft im Hintergrund im Infobereich und zeigt das verbundene Konto. Neue Versionen werden angeboten und im Leerlauf installiert, nicht während eines Schreibvorgangs. Um sofort zu prüfen, wählen Sie im Menü des Infobereichs **Nach Updates suchen**: Eine neue Version öffnet das Fenster mit dem Update, sonst melden Fenster und Tooltip des Symbols, dass die App aktuell ist oder die Prüfung fehlgeschlagen ist. Kapitel 16 erklärt das Beschreiben von Tags.

Unten im Fenster des Dienstprogramms stehen die Version, der Firmenname und Links zu Website, Datenschutzerklärung, Impressum und Support-E-Mail (ein gebrandetes Dienstprogramm zeigt nur die Links seiner Marke). **Lizenzen von Drittanbietern** listet dort die verwendeten Open-Source-Pakete auf (**Als Textdatei öffnen** öffnet die vollständige Liste); ein erneuter Klick blendet die Liste aus. Kann der Computer einen Link nicht öffnen, zeigt das Fenster ihn zum Kopieren an. Oben im Fenster stehen die Adresse und das Konto, mit denen das Dienstprogramm verbunden ist; eine neue Version erscheint dort als Karte mit **Jetzt aktualisieren**.

Unter dem Konto zeigt eine Statuszeile, ob das Dienstprogramm verbunden ist: Sie wird gelb, während es die Verbindung wiederherstellt, und rot, wenn es offline ist; der Tooltip des Symbols im Infobereich zeigt denselben Status und eine neue Version. Beim Start öffnet das Dienstprogramm sein Fenster mit „Verbindung mit … wird hergestellt“, während es sich erneut anmeldet; antwortet der Server nicht, behält es Adresse und Token und bietet **Erneut versuchen** an. Das Menü im Infobereich enthält **Abmelden**, das den gespeicherten Token von diesem Computer entfernt (der Token selbst bleibt gültig), und **Beenden**; solange noch Tags beschrieben werden, fragen beide zuerst nach und warten, bis die laufenden Vorgänge abgeschlossen sind.

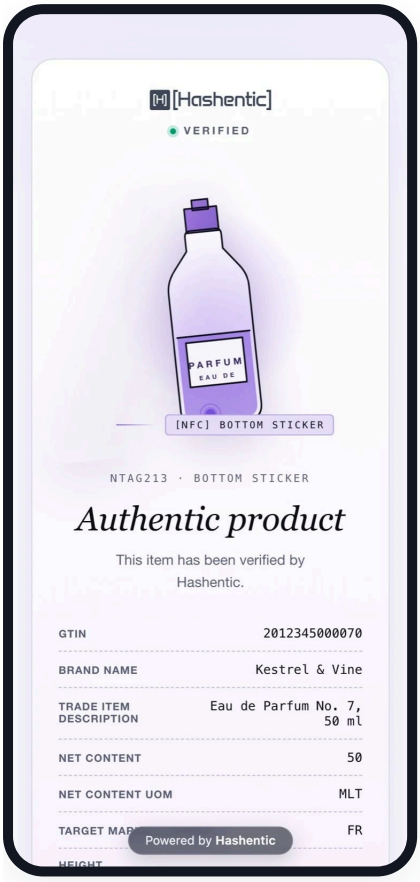
> **Tokens**
>
> Der Desktop application token auf der Applications-Seite meldet das Dienstprogramm mit Ihrem Konto an. **Regenerate** macht den alten Token ungültig und meldet Dienstprogramme ab, die ihn noch verwenden.

> **Lizenzlimits**
>
> Lehnt die Lizenz einen Schreibvorgang ab, nennen beide Apps den Grund statt einer allgemeinen Fehlermeldung. Ist das NFC-Schreib- oder QR-Code-Limit dieses Monats aufgebraucht, nennt die Meldung das Datum, an dem das Limit zurückgesetzt wird; bis dahin kann Ihre Administration im Administrationsbereich zu einem höheren Tarif wechseln oder, sofern der Tarif Pakete anbietet, ein Paket kaufen. Für Gesamtlimits für Tags, QR-Codes oder Produkte älterer Lizenzen und für eine inaktive Lizenz wenden Sie sich an Ihre Administration. Das Desktop-Dienstprogramm zeigt die Meldung in seinem Fenster, ohne Ihrem Browser den Fokus zu nehmen, und entfernt sie nach dem nächsten erfolgreichen Schreibvorgang; der Administrationsbereich zeigt sie ebenfalls.

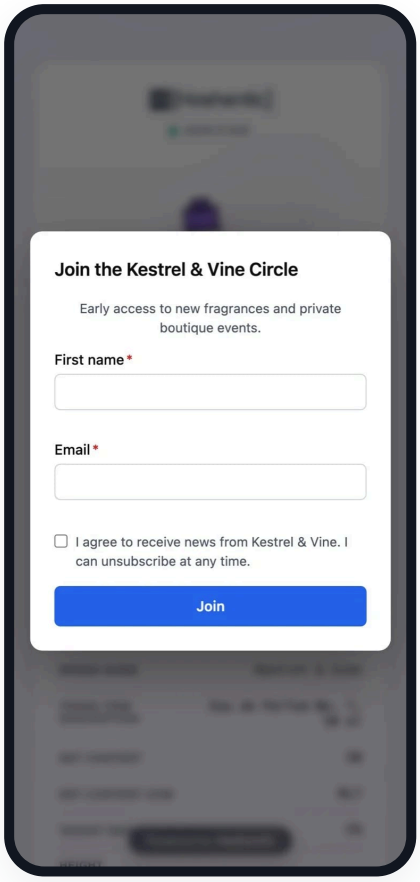
IHRE KUNDEN

23 Die Verifizierungsseite für Verbraucher

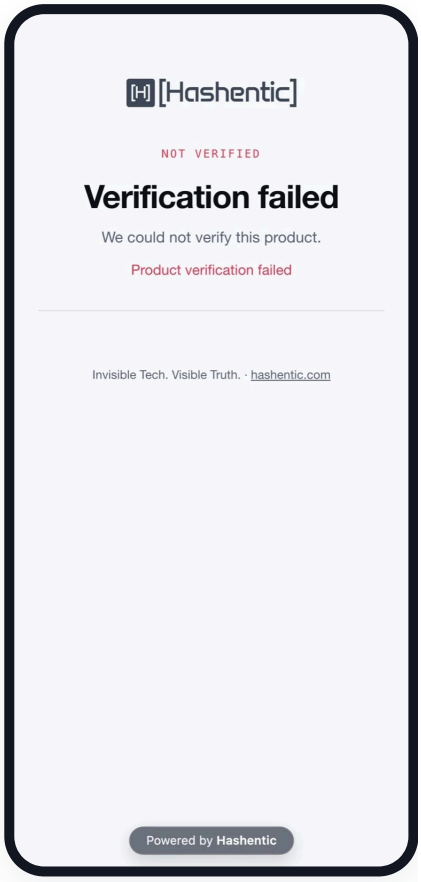
Das Kundenerlebnis nach dem Antippen des Tags oder Scannen des Codes: eine sofortige Antwort im Design Ihrer Marke und ein Grund, auf der Seite zu bleiben.



Verifiziert. Das Galerie-Design Cosmetics mit den Produktfeldern.



Ein Formular nach dem Scan, hier eine Newsletter-Anmeldung mit Einwilligung.



Nicht verifiziert. Für fehlgeschlagene Scans; Gestaltung unter Settings oder je Asset.

Was bei einem Scan geschieht

1. Tag oder Code öffnet Ihren Verifizierungslink. Ein sicherer NFC-Tag ergänzt einen einmaligen kryptografischen Code.
2. Hashentic prüft Produkt, Tag und Zähler und erfasst den Scan mit Zeitpunkt, Standort und Gerät.
3. Kunden sehen die Seite für **gültige Scans** des Assets oder eine **Auth-Vorlage**, die Tag-Typ, Label oder Land entspricht. Fehlgeschlagene Scans zeigen die Seite für **ungültige Scans** oder eine passende **Fehlerseitenregel** für Fehlergrund, Tag-Typ oder Land. Mehrsprachige Seiten öffnen sich in der Browsersprache des Besuchers.
4. Workflows mit *On verify* werden ausgeführt und die Betrugserkennung berücksichtigt den Scan.

Auf der Seite

- **Ihr Design** aus Galerie, Blockeditor, eigenem HTML oder Ihrer Website. Eine Website-Seite zeigt beim Öffnen eine Ladeanzeige. Ist sie nach 10 Sekunden nicht geladen, zeigt eine Karte das Ergebnis (verifiziert oder nicht) und eine Schaltfläche `Open website`, die Ihre Website in einem neuen Tab öffnet.
- **Die Kundensprache**: Übersetzte Vorlagen öffnen sich in der Browsersprache; die integrierte Seite unterstützt die acht Sprachen des Administrationsbereichs.

- **Fragen zum Produkt**: Der KI-Assistent antwortet in der Kundensprache ausschließlich mit öffentlichen Informationen. Er bestätigt selbst keine Echtheit; das übernimmt der Scan. Jede Antwort ist mit "AI-generated answer — may be inaccurate" gekennzeichnet, und ein Hinweis unter dem Eingabefeld bittet Kunden, keine personenbezogenen Daten anzugeben.
- **Botschutz** (Cloudflare Turnstile oder Google reCAPTCHA) schützt KI-Assistent und Formulare, niemals die Verifizierung selbst.
- Schaltfläche **Documents**: öffentliche Handbücher und Zertifikate des Produkts herunterladen.
- **Formulare**: Garantieregistrierung, Anmeldungen, Reparaturanfragen mit Einwilligungsfeldern und Links zu Datenschutz und Bedingungen. Ohne Datenschutz-URL öffnet der Link Privacy Policy der Einwilligung den integrierten Datenschutzhinweis. Ein langes Formular scrollt auf Smartphones innerhalb seines Fensters. Fehlerhafte Eingaben erhalten unter dem Feld eine konkrete Meldung (zum Beispiel "Enter a number from 18 to 99."), die Schaltfläche zeigt beim Senden "Sending…", und eine Meldung "Thank you" bestätigt den Versand. Lehnt der Server das Formular ab, wird seine Meldung statt eines allgemeinen Fehlers angezeigt.
- Link **Privacy** in der Fußzeile: öffnet Ihre Datenschutzerklärung, wenn Sie deren URL im Branding hinterlegt haben. Andernfalls öffnet er einen integrierten Datenschutzhinweis: Ihre Marke ist der Verantwortliche (genannt wird der Markenname aus Branding, falls Sie einen festgelegt haben), Hashentic (XORDEX VENTURES Sp. z o.o.) verarbeitet die Scandaten in Ihrem Auftrag; dazu, was ein Scan erfasst, dass die Seite keine Cookies setzt und dass sich Kunden für ihre Betroffenenrechte an Sie wenden.
- Assistent, Formulare und Datenschutzhinweis unterstützen Englisch, Deutsch, Spanisch, Französisch, Polnisch, Portugiesisch, Russisch und Chinesisch entsprechend dem Browser des Besuchers.
- **Integrierte Fehlerseite**: nennt den Grund, wenn der Link bereits verwendet wurde, und zeigt einen Link `Contact support`, wenn Sie in Branding eine Support-URL hinterlegt haben.
- Schlägt eine Frage an den Assistenten fehl, bleibt sie im Eingabefeld stehen, sodass der Kunde sie erneut senden kann.

> **Wiederholte Scans sicherer Tags**
>
> Jedes Antippen eines NTAG 424 DNA oder EM4425 erzeugt einen neuen Code. Ein zweites Öffnen desselben Links (aus dem Browserverlauf oder einer weitergegebenen Nachricht) schlägt mit "Already verified" fehl. Das schützt vor kopierten Links. Sollen Kunden zur Seite zurückkehren können, aktivieren Sie **Allow already verified asset page**: Gestaltete Seiten werden dann mit dem Hinweis "Product is not verified: this link has already been used." in der Sprache des Besuchers erneut gezeigt (ohne Dokumente, Assistent und Formulare).

III

Schrittanleitungen

Kurze Anleitungen für häufige Aufgaben, von der Kontosicherung bis zur Untersuchung eines Fälschungsalarms. Jede nennt die genauen Schaltflächen.

24 Ihr Konto absichern

25 Eine neue Produktlinie einrichten

26 Die Verifizierungsseite gestalten

27 Die Verifizierungsseite übersetzen

28 Bei fehlgeschlagenen Scans eine andere Seite anzeigen

29 Produkte mit QR-Code anlegen und Etiketten drucken

30 NFC-Tags mit dem Desktop-Dienstprogramm beschreiben

31 Einen Betrugsalarm untersuchen

32 Geklonte Tags automatisch sperren

33 Garantieregistrierungen erfassen

34 Ein Teammitglied hinzufügen

35 Viele Produkte gleichzeitig aktualisieren

36 Die KI bei Kundenantworten unterstützen

37 Die mobile App verbinden

38 Hashentic mit Shopify nutzen

ANLEITUNG · ALLE BENUTZER

24 Ihr Konto absichern

Aktivieren Sie die Zwei-Faktor-Authentifizierung, damit ein gestohlenes Passwort allein keinen Kontozugriff ermöglicht. Sie benötigen zwei Minuten und eine Authenticator-App wie Google Authenticator oder Microsoft Authenticator.

1. Klicken Sie oben rechts auf Ihren Avatar und dann auf **Open profile**.
2. Aktivieren Sie unter **Security** die Option **Activate two-factor authentication**.
3. Scannen Sie den QR-Code mit Ihrer Authenticator-App oder geben Sie den darunter angezeigten Schlüssel in der App ein.
4. Geben Sie den sechsstelligen App-Code unter **Two-factor authentication code** und Ihr **Account password** ein und klicken Sie auf **Send**.
5. Speichern Sie Ihre 10 **Wiederherstellungscodes** mit **Copy all** oder **Download .txt** sicher ab, aktivieren Sie **I have saved my recovery codes** und klicken Sie auf **Done**.

Ab jetzt benötigen Sie bei der Anmeldung einen Code aus der App. Bei Verlust Ihres Telefons verwenden Sie **Use a recovery code instead**; jeder Code funktioniert einmal. In Ihrem Profil können Sie einen neuen Satz erzeugen.

> ✓ **Für die Administration**
>
> Um 2FA für alle verbindlich zu machen, aktivieren Sie **Require 2FA setup** unter System → Settings. Benutzer ohne 2FA werden dann bei ihrer nächsten Anmeldung zur Einrichtung aufgefordert.

ANLEITUNG · KATALOGVERWALTUNG

25 Eine neue Produktlinie einrichten

Bevor das erste Produkt gekennzeichnet werden kann, muss Hashentic die Struktur der Produktlinie kennen. Wir richten die Uhr Heritage Chronograph aus den Beispielen ein.

1. Gemeinsame Listen vorbereiten (optional)

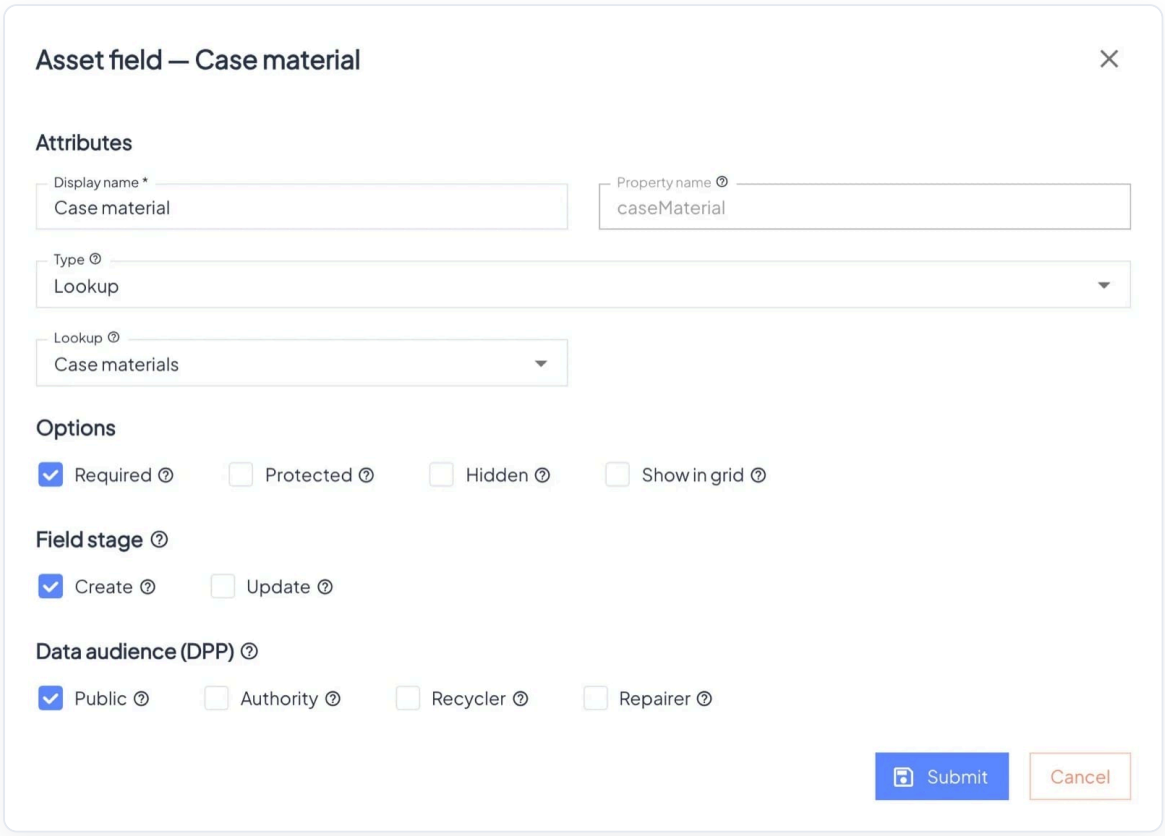
1. Öffnen Sie **Catalog** → **Lookups** und klicken Sie auf **Create lookup**. Benennen Sie die Liste, zum Beispiel *Gehäusematerialien*.
2. Öffnen Sie den Lookup und klicken Sie auf **Create item**. Ergänzen Sie Einträge einzeln oder wechseln Sie zu **Multiple mode** und laden Sie eine CSV- oder Excel-Datei mit Spalten für Wert, Bezeichnung und Beschreibung hoch (Multiple mode benötigt die Lizenzfunktion Bulk write und die Berechtigung Write products).

2. Das Asset erstellen

1. Öffnen Sie **Catalog** → **Assets** und klicken Sie auf **Create asset**.
2. Geben Sie **Name** und **Description** ein. Bei einer festen Auflage tragen Sie **Amount** ein und aktivieren **Limited**. Haben Sie bereits ein Preset für diese Produktart, wählen Sie es unter **Use preset**.
3. Aktivieren Sie **GS1 compliant** für GTINs und GS1 Digital Link oder **DPP compliant** für einen Digitalen Produktpass und schließen Sie die zusätzlichen Schritte ab.
4. Klicken Sie auf **Create**. Die Asset-Seite öffnet sich.

3. Die Felder definieren

1. Öffnen Sie den Tab **Fields** und ergänzen Sie für jede Angabe ein Feld, etwa *Seriennummer* (Text, Required, Show in grid), *Gehäusematerial* (Lookup) oder *Produktionsdatum* (Date, nur vergangene Daten).
2. Wählen Sie die **Field stage**: **Create** für bei der Produktion bekannte Daten, **Update** für später ergänzte Angaben wie *Verkaufsort*.
3. Aktivieren Sie **Protected** für personenbezogene Daten und **Hidden** für Angaben, die Kunden nicht sehen sollen.



Ein Lookup-Feld bezieht seine Werte aus der Liste *Gehäusematerialien*.

4. Die Schutzregeln festlegen

1. Tragen Sie im Tab **Settings** unter **Authorized regions** die Verkaufsländer der Linie ein, damit Graumarkt-Scans Alarme auslösen.
2. Aktivieren Sie optional **Answer customer questions with AI** und schreiben Sie einen Begrüßungstext.
3. Ergänzen Sie unter **Labels** die später benötigten Labels, etwa *Boutique stock* und *Sold*.

✓ **Wiederverwenden**

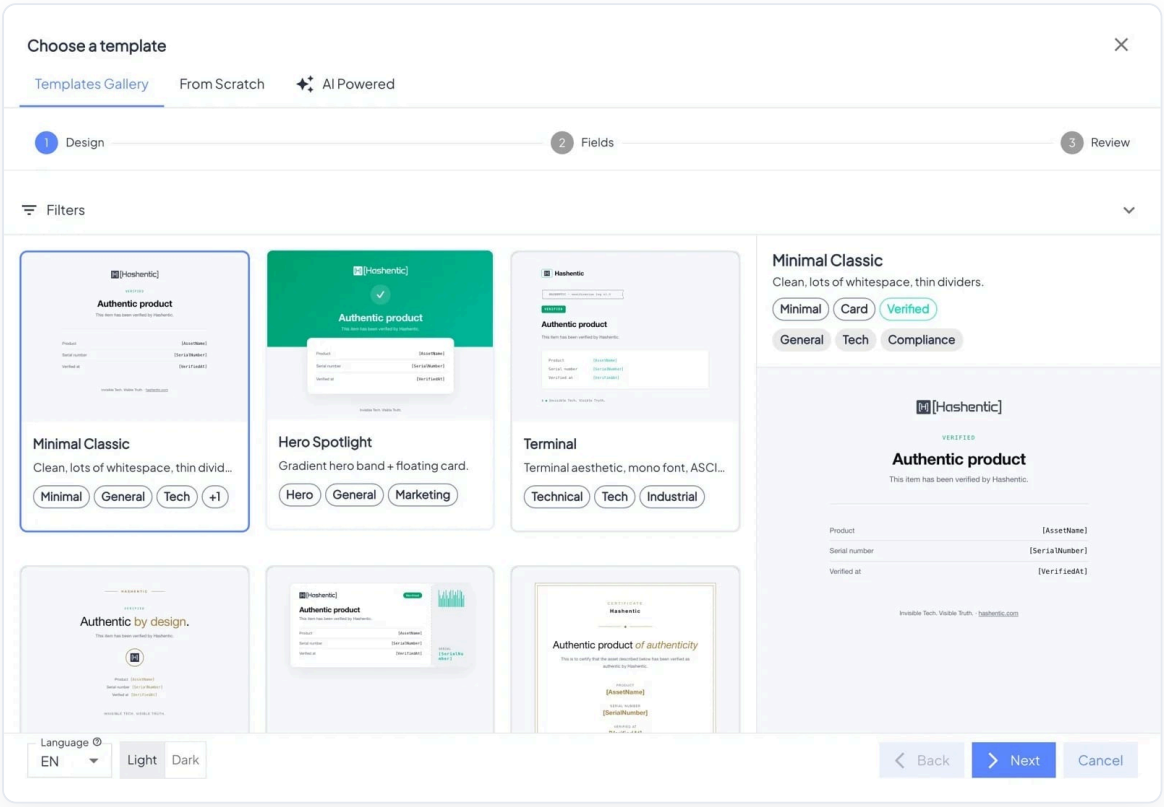
Sind Sie mit der Struktur zufrieden? Bilden Sie sie unter **Catalog** → **Presets** als Preset nach und wählen Sie es beim nächsten ähnlichen Asset aus.

ANLEITUNG · MARKETING

26 Die Verifizierungsseite gestalten

Wählen Sie ein Design aus der Galerie, legen Sie die angezeigten Inhalte fest und prüfen Sie die Vorschau, bevor Kunden die Seite sehen.

1. Öffnen Sie das Asset und wechseln Sie zum Tab **Templates**. Klicken Sie unter **Verified page template** auf **Choose a template**.

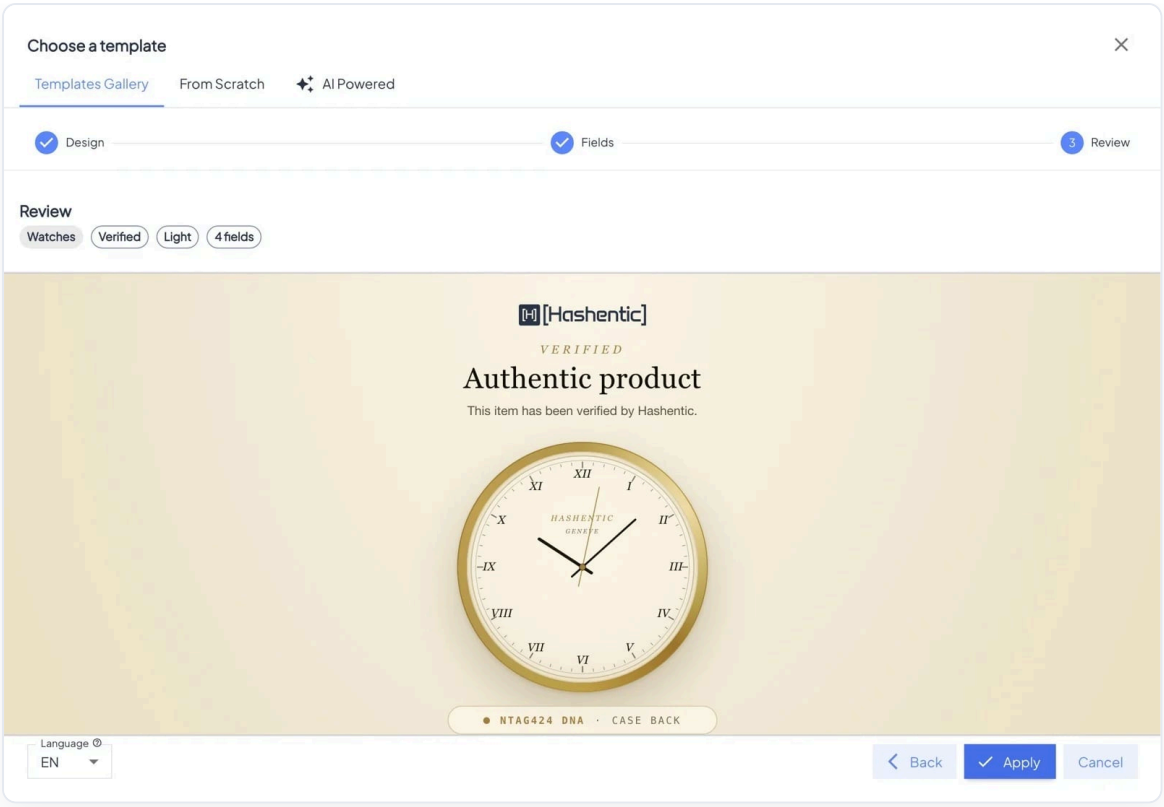


Die Galerie. Öffnen Sie **Filters**, um zu suchen oder nach Stil, Anwendungsfall und Layout zu filtern.

2. Klicken Sie auf ein Design, um seine Vorschau zu öffnen. Wechseln Sie zwischen **Light** und **Dark** sowie zwischen den Seitensprachen und klicken Sie auf **Next**.

3. Aktivieren Sie im Schritt **Fields** die gewünschten Felder und ordnen Sie sie mit den Pfeilen an. **Smart defaults** wählt eine sinnvolle Zusammenstellung. Klicken Sie auf **Next**.

4. Prüfen Sie unter **Review** das Ergebnis und klicken Sie auf **Apply**.



Prüfschritt: die Uhrenseite mit den ausgewählten Feldern.

5. Optional: Legen Sie mit **Button color** die Farbe der Dokument- und Assistentenschaltflächen fest oder passen Sie mit **Edit Template** Texte und Bilder im Blockeditor an.
6. Behalten Sie für fehlgeschlagene Scans **Use global template** bei (unter System → Settings gestaltet) oder entwerfen Sie eine eigene Seite für dieses Asset.
7. Prüfen Sie das Ergebnis an einem beliebigen Produkt: Öffnen Sie es und klicken Sie auf **Preview**.

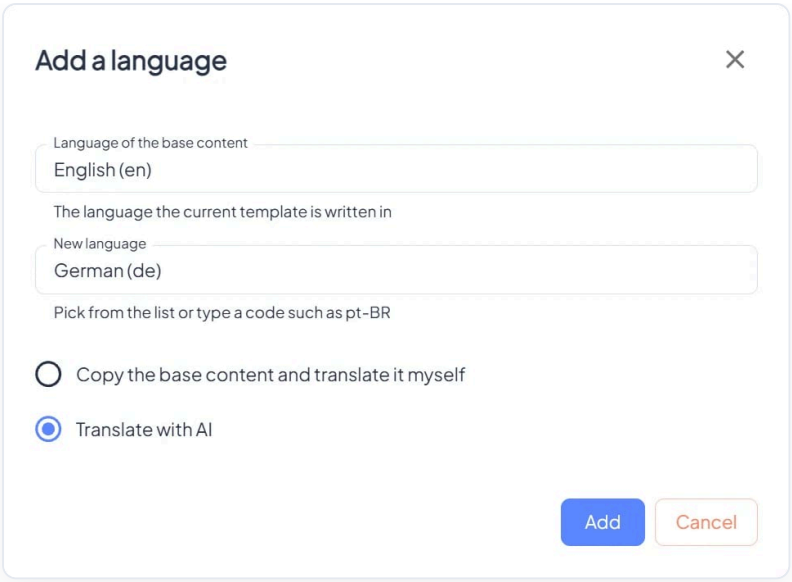
> **Unterschiedliche Seiten für unterschiedliche Scans**
> Im Tab **Auth templates** fügt **New template** eine Seite hinzu, die nur für bestimmte Tag-Typen, Labels oder Länder gilt, etwa einen Hinweis bei Scans außerhalb Ihrer Märkte oder eine Mitarbeiterseite für Produkte mit dem Label *Boutique stock*.

ANLEITUNG · MARKETING

27 Die Verifizierungsseite übersetzen

Zeigen Sie die Produktseite in den Sprachen Ihrer Kunden. KI erstellt einen Übersetzungsentwurf, den Sie prüfen und speichern.

1. Öffnen Sie das Asset und den Tab **Templates**. Speichern Sie zuerst die Vorlage für gültige Scans, falls Sie sie geändert haben.
2. Klicken Sie in der Leiste **Languages** unter der Vorlage auf **Add language**.
3. Legen Sie beim ersten Mal **Language of the base content** fest: die Sprache, in der die Vorlage aktuell verfasst ist.
4. Wählen Sie **New language** aus der Liste oder geben Sie einen Code wie `pt-BR` ein.
5. Wählen Sie **Translate the base template with AI** und klicken Sie auf **Add**. Soll diese Sprache stattdessen ein eigenes Design erhalten, wählen Sie **Choose a different template** und klicken Sie auf **Choose a template**: Übernehmen Sie ein Design aus der Galerie, beginnen Sie bei null oder lassen Sie eines von der KI erstellen, genau wie bei der Basisvorlage.



Deutsch zu einer englischen Vorlage hinzufügen.

6. Öffnen Sie die neue Sprache und klicken Sie auf **Edit**, um Produktnamen, Aussagen und Rechtstexte zu prüfen. Speichern Sie.
7. Wiederholen Sie dies für die Seite ungültiger Scans und jede Auth-Vorlage sowie jede Regel für fehlgeschlagene Scans, die Ihre Kunden sehen können.
8. Testen Sie das Ergebnis: Stellen Sie Ihr Telefon oder Ihren Browser auf diese Sprache und scannen Sie ein Produkt.

✓ **Wenn sich die Basisseite ändert**

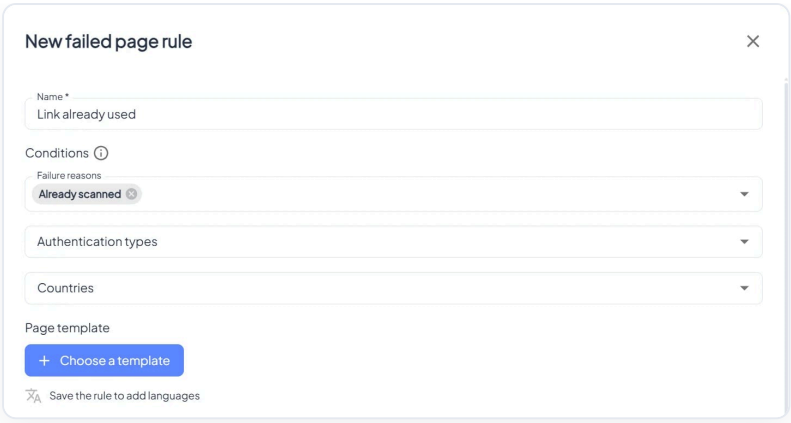
Sprachen sind separate Kopien. Öffnen Sie nach einer Änderung der Basisvorlage jede Sprache und klicken Sie auf **Translate the base template with AI** (dies ersetzt Ihre Änderungen in dieser Sprache), bearbeiten Sie sie manuell oder geben Sie ihr mit **Replace template** ein neues Design.

ANLEITUNG · MARKENSCHUTZ

28 Bei fehlgeschlagenen Scans eine andere Seite anzeigen

Erklären Sie Kunden verständlich, was passiert ist: Ein wiederverwendeter Link, ein zurückgezogenes Produkt und ein Fälschungsverdacht erhalten jeweils eine eigene Seite.

1. Öffnen Sie das Asset, wechseln Sie zu **Auth templates** und scrollen Sie zu **Failed page rules**. Klicken Sie auf **New rule**.
2. Benennen Sie die Regel, etwa *Link bereits verwendet*. Wählen Sie unter **Failure reasons** die Option **Already scanned**.



Die Regel für bereits verwendete Links.

3. Gestalten Sie unter **Page template** die Seite, etwa: "Dieser Link wurde bereits verwendet. Halten Sie Ihr Telefon erneut an den Tag, um das Produkt zu prüfen." Speichern Sie.
4. Fügen Sie eine Regel *Zurückgezogenes Produkt* für **Blocked or withdrawn** hinzu und nennen Sie auf der Seite Ihren Servicekontakt.
5. Ergänzen Sie eine Regel für **Authentication failed** mit einer Warnung und einer Meldemöglichkeit für vermutete Kopien. Beschränken Sie sie mit **Countries**, wenn der Kontakt je Markt abweicht.
6. Ordnen Sie die Regeln durch Ziehen. Die erste passende Regel gilt; trifft keine zu, erscheint die Seite für ungültige Scans des Assets.
7. Ergänzen Sie bei Bedarf Sprachen für jede Regelseite (Die Verifizierungsseite übersetzen).
8. Um Regeln für alle Produktlinien gleichzeitig anzulegen, fügen Sie sie unter System → Settings unterhalb der globalen Vorlage für ungültige Scans hinzu.

> **Wiederholte Scans sicherer Tags**
>
> Ist **Allow already verified asset page** aktiviert, zeigen wiederholte Scans weiterhin die Produktseite mit einem Hinweis; die Regel *Already scanned* greift dann nicht. In eigenem HTML können Sie die Fehlergruppe außerdem über den Platzhalter **[FailReason]** auslesen (Anhang B).

ANLEITUNG · BETRIEB

29 Produkte mit QR-Code anlegen und Etiketten drucken

Erstellen Sie eine Produktcharge aus einer Tabelle und drucken Sie einen Bogen QR-Codes ganz ohne Spezialhardware.

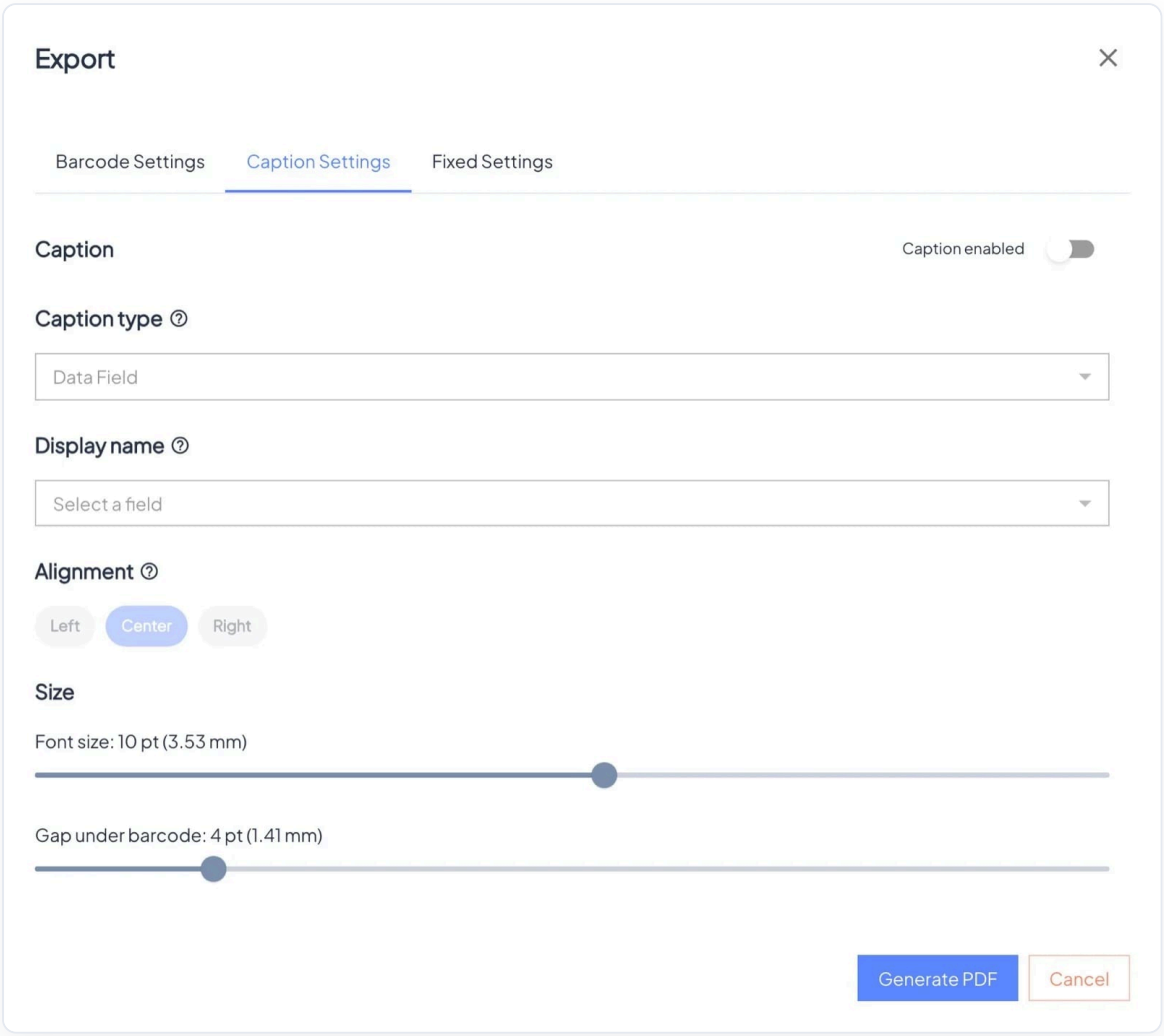
Lizenz Bulk write für die Schritte 2–7

1. Bereiten Sie eine CSV- oder Excel-Datei mit einer Zeile pro Produkt vor. Benennen Sie die Spalten wie die Asset-Felder (Eigenschaftsnamen wie **batchNumber**); sie werden automatisch zugeordnet.
2. Öffnen Sie **Catalog** → **Products** → **Add new**, wählen Sie **Barcode** und den Tab **Multiple mode**.
3. Wählen Sie das Asset unter **Asset name**, dann **Upload file** und Ihre Datei. (Keine individuellen Produktdaten? Wählen Sie **Generate by number** und geben Sie eine Anzahl ein.)
4. Klicken Sie auf **Next**. Prüfen Sie unter **Set up fields**, dass jedes Feld der richtigen Spalte zugeordnet ist, und klicken Sie erneut auf **Next**.

5. Korrigieren Sie markierte Zeilen mit dem Bearbeitungssymbol und klicken Sie auf **Generate**. Die Codes werden im Hintergrund angelegt; Sie können den Dialog schließen.

6. Öffnen Sie **Operations** → **Bulk operations**. Sobald der Durchlauf *Completed* anzeigt, klicken Sie auf **Download barcodes**.

7. Wählen Sie unter **Export** die Optionen **PDF**, **QRCode** und die URL-Version **Public**, legen Sie eine Größe fest (Medium passt für die meisten Etiketten) und wählen Sie unter **Caption settings** ein Feld wie die Chargennummer als Beschriftung unter jedem Code. Prüfen Sie das Raster unter **Fixed settings** und klicken Sie auf **Generate PDF**.



Beschriftungseinstellungen: ein Feldwert oder eigener Text unter jedem Code.

QR-Codes gestalten

Für QR-Codes im PDF legt der Tab **Design** Code- und Hintergrundfarbe fest, quadratische, abgerundete oder Punkt-Module, die Form der Eckmarkierungen und ein Logo in der Mitte: Ihr Markenlogo oder ein hochgeladenes Bild, in drei Größen. Die Vorschau aktualisiert sich bei jeder Änderung, und die Einstellungen werden auf Ihrem Gerät gespeichert. Hashentic lehnt Farben ab, die Scanner nicht lesen können, etwa einen hellen Code auf dunklem Hintergrund. Geben Sie Farben als #RRGGBB ein oder nutzen Sie die Farbauswahl. Ein hochgeladenes Logo (PNG, JPG, WebP oder SVG, bis 2 MB) wird auf die für ein Etikett nötige Größe verkleinert. Punkt- und abgerundete Module machen das PDF größer: Ein Export mit mehr als 15 000 Codes bei **Dots** oder 30 000 bei **Rounded** druckt quadratische Module; Farben, Eckmarkierungen und Logo bleiben erhalten, und der Dialog weist darauf hin. Exportieren Sie kleinere Stapel, um den Stil zu behalten. Scannen Sie die Vorschau mit einem Telefon, bevor Sie eine große Serie drucken.

Einzelne Produkte

Verwenden Sie für ein Produkt **Single mode**: Werte ausfüllen, auf **Write** klicken und anschließend auf der Produktseite auf **Download**. **Clone count** druckt mehrere Kopien desselben Codes.

ANLEITUNG · PRODUKTION

30 NFC-Tags mit dem Desktop-Dienstprogramm beschreiben

Sichere NFC-Tags werden an Ihrer Produktions- oder Verpackungsstation mit einem USB-Lesegerät beschrieben. Sie benötigen das Desktop-Dienstprogramm, ein USB-NFC-Lesegerät und leere Tags.

Einmalig installieren und verbinden

1. Klicken Sie im Menü auf **Setup desktop utility**, prüfen Sie **Your platform** und klicken Sie auf **Download for …**. Führen Sie das Installationsprogramm aus.
2. Klicken Sie im Dialog auf **Register desktop utility**. Das Dienstprogramm öffnet sich und meldet sich mit Ihrem Konto an. (Alternativ kopieren Sie den **Desktop application token** aus System → Applications in das Dienstprogramm.)
3. Nach der Anmeldung wird die obere Schaltfläche grün: **Connected**. Schließen Sie dann das Lesegerät an; der Dialog zum Hinzufügen von Produkten weist auf ein fehlendes Lesegerät hin.

Einen Tag beschreiben

1. Öffnen Sie **Products** → **Add new**, behalten Sie **NFC Tag** und **Single mode** bei und wählen Sie das Asset.
2. Legen Sie einen Tag auf das Lesegerät. Der Administrationsbereich zeigt seinen Typ an.
3. Geben Sie die Produktwerte ein und klicken Sie auf **Write**. Warten Sie auf "Tag written."; die Seite des neuen Produkts öffnet sich.

Eine Charge beschreiben

1. Wechseln Sie zu **Multiple mode**, wählen Sie das Asset und laden Sie Ihre Datei hoch (oder rufen Sie Datensätze aus Ihrem ERP ab). Lassen Sie **Save import** aktiviert.
2. Ordnen Sie die Felder zu, korrigieren Sie markierte Zeilen und klicken Sie auf **Generate**.
3. Legen Sie den ersten Tag auf, warten Sie bis zum Abschluss, entfernen Sie ihn und legen Sie den nächsten auf. Fortschritt und Fehler erscheinen je Zeile; verwenden Sie am Ende **Retry failed**.
4. Unterbrochen? Öffnen Sie dasselbe Asset erneut im Multiple mode und klicken Sie auf **Proceed**, um fortzufahren.

Das Schreiben stoppt, wenn das NFC-Tag-Limit dieses Monats aufgebraucht ist: Administrationsbereich, mobile App und Desktop-Dienstprogramm zeigen *Monthly NFC tag limit reached* (siehe Monatslimits und Pakete).

> **Wenn die Schaltfläche "Connect application" anzeigt**
>
> Das Dienstprogramm läuft nicht oder ist nicht mit Ihrem Konto angemeldet. Klicken Sie auf die Schaltfläche, um es zu starten. Besteht weiterhin keine Verbindung, öffnen Sie sein Fenster über den Infobereich oder registrieren Sie es erneut im Einrichtungsdialog. Nach der Verbindung können Sie seine Protokolle für den Support im Menü der oberen Schaltfläche herunterladen (**Download logs**).

ANLEITUNG · MARKENSCHUTZ

31 Einen Betrugsalarm untersuchen

Ein Critical-Alarm ist eingegangen: Dieselbe Uhr wurde in Paris und zwei Stunden später in Istanbul gescannt, mit einem älteren Tag-Zählerstand. So gehen Sie vor.

1. Öffnen Sie **Analytics** → **Fraud alerts**. Grenzen Sie die Auswahl mit **Add filter** → **Status** = New und **Severity** = Critical ein.
2. Klicken Sie auf den Alarm. Lesen Sie die **Signals** (hier *Cloned chip* und *Impossible travel*), **Metrics** (Entfernung, Geschwindigkeit, Zählerstände) und **Triggering scans**.
3. Klicken Sie auf **Acknowledge**, damit Kollegen wissen, dass Sie den Fall bearbeiten.
4. Öffnen Sie **Verifications**, suchen Sie die Produktkennung und öffnen Sie über das Uhrsymbol die vollständige **Verification history** des Tags: wo und auf welchen Geräten er gescannt wurde.
5. Bestätigen die Hinweise den Verdacht, öffnen Sie das Produkt, wechseln Sie zu **Authentications** und wählen Sie beim geklonten Tag **Block authentication**. Jeder spätere Scan schlägt fehl. (Das Sperren des gesamten Produkts auf seiner Seite erfordert das Einlesen des echten Tags, sofern das Asset keine ungeschützte Verwaltung erlaubt.)
6. Klicken Sie im Alarm auf **Confirm fraud**. War es ein Fehlalarm, etwa ein reisender Kunde mit VPN, klicken Sie auf **Dismiss**.

✓ **Den Zusammenhang prüfen**

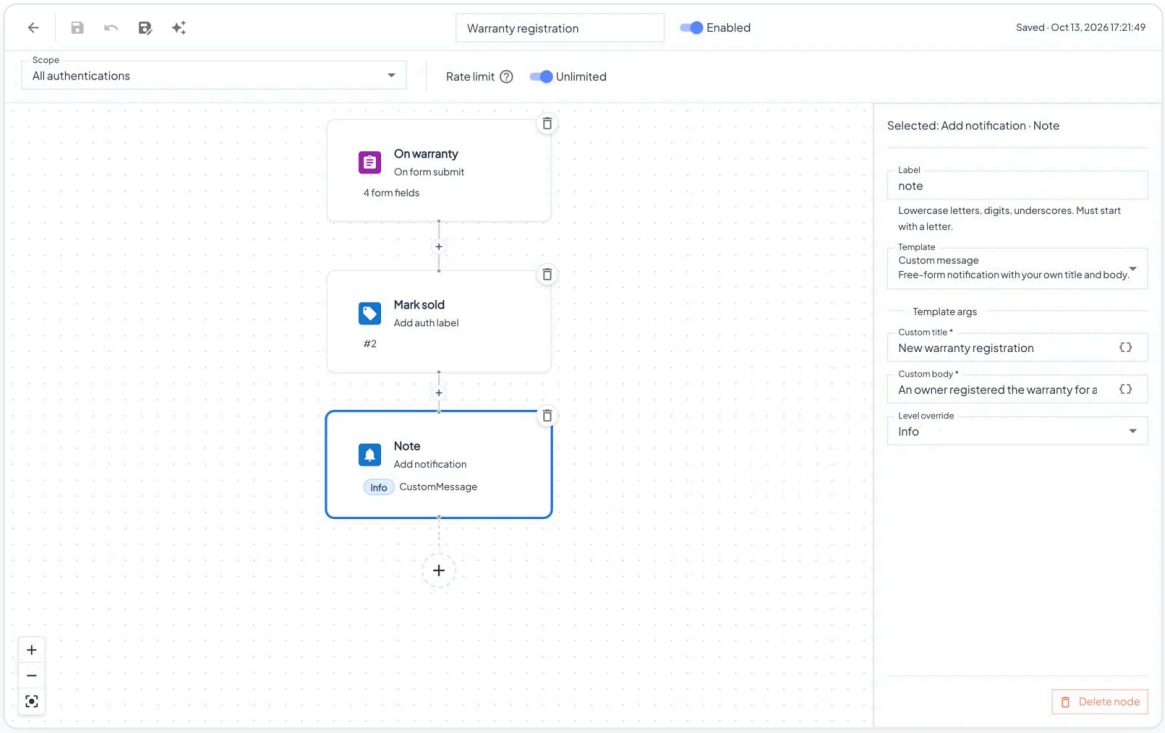
Aktivieren Sie auf der **Geo map** die Optionen **Invalid** und **Risky**, um örtliche Häufungen fehlgeschlagener Scans zu erkennen. Am Asset kann **AI analysis** Veränderungen zusammenfassen: "Gibt es Betrugsrisiken, die ich prüfen sollte?"

ANLEITUNG · AUTOMATISIERUNG

32 Geklonte Tags automatisch sperren

Lassen Sie Hashentic selbst reagieren, wenn die Betrugserkennung sicher ist: den Tag sperren und das Team alarmieren, zu jeder Tageszeit.

1. Öffnen Sie das Asset, den Tab **Workflows** und klicken Sie auf **New workflow**. Nennen Sie ihn *Reaktion auf Fälschungen*.
2. Klicken Sie auf **Add a trigger** und wählen Sie **On fraud detected**. Setzen Sie in den Eigenschaften **Minimum severity** auf *High*.
3. Klicken Sie auf **Add step** → **Add notification**. Wählen Sie die Vorlage *Custom message*, schreiben Sie Titel und Text und setzen Sie **Level override** auf *Critical*.
4. Ergänzen Sie einen weiteren Schritt: **Block authentication**.
5. Stellen Sie sicher, dass **Enabled** aktiv ist, und klicken Sie auf **Save**.



Einen Schritt bearbeiten: der Eigenschaftenbereich rechts.

Bei jedem High- oder Critical-Alarm für dieses Asset wird der Workflow ausgeführt. **Block authentication** greift nur bei Alarmen zu einem bestimmten Tag (geklonter Chip, unmögliche Reise, Scanrate). Bei Graumarkt- und Fehlscan-Häufungsalarmen wird der Schritt übersprungen; die Benachrichtigung wird dennoch versandt. Öffnen Sie in der Liste die Anzahl der Durchläufe, um jeden Durchlauf, das betroffene Produkt und das Ergebnis jedes Schritts zu sehen.

> **Lieber eine fertige Vorlage?**
> **From template…** → *Anti-counterfeit: block on second scan* sperrt ein Produkt beim zweiten Scan und benachrichtigt Sie. Das eignet sich für Einwegartikel wie versiegelte Verpackungen.

ANLEITUNG · KUNDENSERVICE

33 Garantieregistrierungen erfassen

Machen Sie aus der Verifizierung eine Kundenregistrierung: ein kurzes Formular nach dem Scan und eine Kennzeichnung des Produkts als verkauft.

1. Öffnen Sie den Tab **Forms** des Assets und klicken Sie auf **New form**.
2. Ergänzen Sie im Formulardesigner eine Überschrift und eine Textzeile sowie die Felder *Vollständiger Name* (Text), *E-Mail*, *Gekauft bei* (Lookup Ihrer Boutiquen) und *Kaufdatum* (Date). Aktivieren Sie im Einstellungsbereich unter **GDPR consent** das Einwilligungsfeld und tragen Sie Text und Version ein.
3. Benennen Sie das Formular, setzen Sie **Show this form to** auf *All authentications*, aktivieren Sie **Allow only one submission per authentication** und **Allow the customer to skip this form** und speichern Sie.
4. Öffnen Sie **Workflows** → **New workflow**. Auslöser: **On form submit**, wählen Sie Ihr Formular. Ergänzen Sie **Add auth label** → *Sold* und **Add notification** für Ihr Kundenserviceteam. Speichern Sie.
5. Scannen Sie ein Produkt: Das Formular erscheint auf der Verifizierungsseite. Einsendungen werden in der Formularzeile aufgelistet; **Download submissions (CSV)** exportiert sie.

Datenschutz

Markieren Sie personenbezogene Felder wie die E-Mail-Adresse auf dem Asset als **Protected**, wenn Sie sie auch am Produkt speichern. Hinterlegen Sie unter Branding die URLs Ihrer Datenschutzerklärung und Bedingungen, damit das Einwilligungsfeld darauf verlinkt.

ANLEITUNG · ADMINISTRATION

34 Ein Teammitglied hinzufügen

Beispiel: Lucas betreut die Verpackungsstation. Er muss Produkte anlegen und kennzeichnen, jedoch keine Einstellungen ändern oder Kundenfragen einsehen.

1. Öffnen Sie **System** → **Users** und klicken Sie auf **Create user**.
2. Geben Sie einen **Username** (zum Beispiel *lucas.meyer*), seine **Email** und ein anfängliches **Password** ein (mindestens 12 Zeichen, darunter ein Buchstabe und eine Ziffer).
3. Wählen Sie unter **Role** die Rolle *User* und belassen Sie den Status auf *Active*.
4. Aktivieren Sie die benötigten Berechtigungen: Read assets and lookups; Read, Write und Update products; Read und Write bulk operations; Read verifications.
5. Wählen Sie unter **Allowed assets** die Produktlinien aus, an denen er arbeitet, und klicken Sie auf **Create**.
6. Übermitteln Sie Lucas seinen Benutzernamen und das Startpasswort über einen sicheren Kanal und bitten Sie ihn, die Zwei-Faktor-Authentifizierung einzurichten.

Wer sieht was?

Admins sehen alle Assets; Users nur ihre erlaubten Assets. Das Audit-Protokoll ist dem Super User vorbehalten. Um den Zugriff zu entziehen, setzen Sie das Konto auf *Inactive* (die Daten bleiben erhalten) oder löschen Sie es.

ANLEITUNG · BETRIEB

35 Viele Produkte gleichzeitig aktualisieren

Beispiel: 40 Kartenetuis wurden in den Pop-up-Store verlegt und ihr *Retail status* muss geändert werden. Felder benötigen die Stufe *Update*, damit sie bearbeitbar sind.

1. Öffnen Sie **Catalog** → **Products** → **Update** und wechseln Sie zu **Multiple mode**.
2. Stellen Sie die Produkte zusammen:
   - **Scan**: Scannen Sie den QR-Code jedes Produkts mit der Webcam oder halten Sie Tags an das Lesegerät. Mit **Import from queue** übernehmen Sie Produkte, die ein Kollege mit der mobilen App gescannt hat.
   - **Query**: Wählen Sie das Asset und filtern Sie die Produkte (nach Label, Datum, Typ …). Angeboten werden nur Assets mit *Allow unprotected management*.
3. Klicken Sie auf **Continue to values**. Legen Sie unter **Shared values** den neuen Wert für alle fest; überschreiben Sie bei Bedarf einzelne Zeilen. Klicken Sie auf **Continue to review**.
4. Prüfen Sie die Liste und klicken Sie auf **Start update**. Die Aktualisierung läuft im Hintergrund und erscheint unter **Bulk operations**. Dort können Sie fehlgeschlagene Vorgänge erneut versuchen.

ANLEITUNG · KUNDENSERVICE

36 Die KI bei Kundenantworten unterstützen

Der Assistent auf der Verifizierungsseite ist auf Ihre Informationen angewiesen. Nutzen Sie Kundenfragen, um Wissenslücken zu schließen.

1. Aktivieren Sie die Funktion: **System** → **Settings** → **Answer customer questions on the verification page**. Aktivieren Sie danach auf jedem Asset unter **Settings** die Option **Answer customer questions with AI** und schreiben Sie einen Begrüßungstext.
2. Öffnen Sie nach einer Woche **Analytics** → **Customer questions** und klicken Sie auf die Kachel **No information**. Diese Fragen konnten Ihre Daten nicht beantworten.
3. Gruppieren Sie die Lücken: Pflegehinweise, Garantiebedingungen, Inhaltsstoffe, Wartung.
4. Laden Sie die Antworten hoch: Klicken Sie im Tab **Documents** des Assets (oder unter **Settings** → **Brand documents** für markenweite Themen) auf **Upload** und fügen Sie eine PDF-, DOCX-, TXT- oder Markdown-Datei hinzu.
5. Wählen Sie in der Dokumentzeile **Edit**, setzen Sie **Audience** auf *Public*, legen Sie die Sprache fest und speichern Sie. Warten Sie, bis der Status *Indexed* erscheint.
6. Prüfen Sie regelmäßig **Thumbs down**: Diese Antworten haben Kunden nicht geholfen.

> **Was der Assistent nicht übernimmt**
>
> Er antwortet ausschließlich aus öffentlichen Produktdaten und öffentlichen Dokumenten, in der Sprache der Frage. Er bestätigt keine Echtheit (das übernimmt der Scan), behandelt keine sachfremden Themen und verarbeitet keine personenbezogenen Daten.

ANLEITUNG · AUSSENDIENST

37 Die mobile App verbinden

Melden Sie sich in Sekunden auf Ihrem Telefon an, indem Sie einen Code im Administrationsbereich scannen. Serveradressen oder Passwörter müssen Sie nicht eintippen.

1. Installieren Sie die Hashentic-App auf Ihrem Telefon. Für Android finden Sie den Download im Administrationsbereich: Menü → **Mobile app** → **Download APK**; alternativ scannen Sie den dort angezeigten Code.
2. Öffnen Sie im Administrationsbereich **System** → **Applications** und klicken Sie unter **Sign in on mobile** auf **Show QR code**.
3. Tippen Sie auf dem Telefon auf **Staff sign-in** → **Sign in by scanning QR**, erlauben Sie den Kamerazugriff und scannen Sie den Code. Er ist bis zu zwei Minuten gültig (ein neuer erscheint automatisch) und kann nur einmal verwendet werden.
4. Falls Ihr Konto die Zwei-Faktor-Authentifizierung nutzt, geben Sie den Code auf dem Telefon ein. Die Webseite bestätigt: "Successfully signed in on your phone."
5. Empfehlung: Schützen Sie die App unter **App lock** mit einer PIN oder Face ID.

Sie können jetzt Produkte scannen, suchen, ihre Daten bearbeiten und NFC-Tags mit dem Telefon beschreiben. Um ein bestimmtes Produkt zu öffnen, scannen Sie den **QR for the mobile app** auf seiner Seite im Administrationsbereich.

ANLEITUNG · SHOPIFY

38 Hashentic mit Shopify nutzen

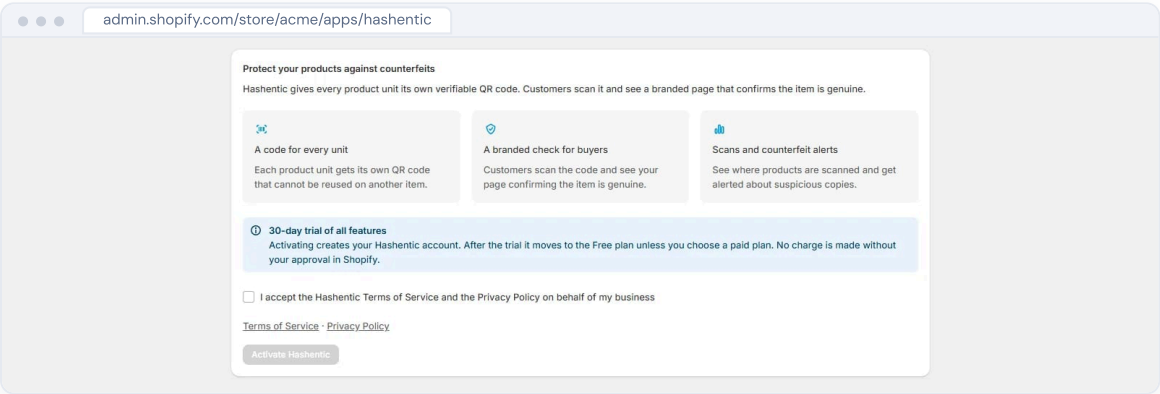
Installieren Sie die Hashentic-App aus dem Shopify App Store, schützen Sie Ihre Produkte, erhalten Sie für jede verkaufte Einheit einen QR-Code und zeigen Sie auf Ihren Produktseiten einen Block „Echtheit prüfen“.

Ort Shopify-Adminbereich → Apps → Hashentic

Die Shopify-App legt ein Hashentic-Konto für Ihren Shop an und betreibt es. Alles, was Sie in der App tun, erscheint auch in Ihrem Hashentic-Administrationsbereich, der für die weiteren Funktionen (Seitenvorlagen, Fälschungswarnungen, Workflows, NFC-Tags) verfügbar bleibt. Die App folgt der Sprache Ihres Shopify-Adminbereichs: Englisch, Deutsch, Spanisch, Französisch, Polnisch, Portugiesisch, Russisch oder Chinesisch, bei jeder anderen Sprache Englisch.

Aktivieren

1. Installieren Sie **Hashentic** aus dem Shopify App Store und öffnen Sie die App unter **Apps** in Ihrem Shopify-Adminbereich.
2. Lesen Sie die Nutzungsbedingungen und die Datenschutzerklärung, setzen Sie das Häkchen und klicken Sie auf **Hashentic aktivieren**. Mit der Aktivierung akzeptieren Sie die Bedingungen für Ihr Unternehmen, deshalb kann das nur der Shopinhaber tun; Mitarbeiter sehen einen Hinweis, sich an den Inhaber zu wenden.
3. Warten Sie ein bis drei Minuten, während Ihr Konto angelegt wird. Die App zeigt jeden Schritt; Sie können die Seite verlassen.



Aktivieren. Die Bedingungen einmal akzeptieren; das Konto wird im Hintergrund angelegt.

Dauert die Einrichtung länger als 10 Minuten, zeigt die Startseite die Warnung **Die Einrichtung dauert länger als üblich**. Sie müssen nichts tun: Die Einrichtung versucht es im Hintergrund weiter. Ist das Konto nach einer Stunde noch nicht bereit, nutzen Sie den Support-Link in der Warnung.

Sobald das Konto bereit ist, zeigt die Startseite die Checkliste **Erste Schritte** mit den nächsten Schritten.

Ihr Konto startet mit einer Testphase (30 Tage, sofern nicht anders festgelegt) und wechselt danach in den Free-Tarif, sofern Sie keinen kostenpflichtigen Tarif wählen. Seine Adresse ist Ihr Shopname mit einem kurzen zufälligen Zusatz, zum Beispiel `acme-k7mq.hashentic.com`. Bekannte Markennamen erhalten eine neutrale Adresse. Für Ihren Markennamen öffnen Sie **Einstellungen** und klicken auf den Link **Fordern Sie eine eigene Subdomain an**; wir prüfen die Anfrage von Hand.

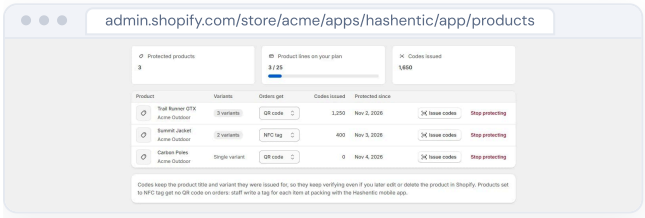
Der Shopinhaber erhält eine Willkommens-E-Mail mit den Zugangsdaten für den Hashentic-Administrationsbereich.

Produkte schützen und Codes ausgeben

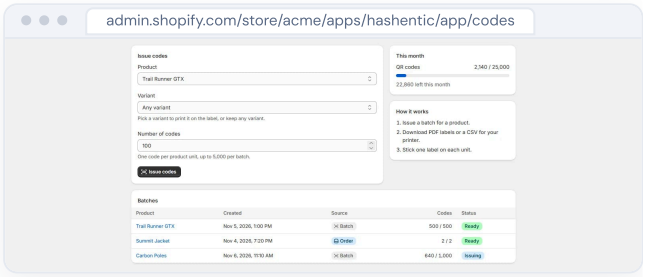
1. Öffnen Sie **Geschützte Produkte** und klicken Sie auf **Produkte schützen**. Wählen Sie bis zu 50 Produkte auf einmal in der Shopify-Produktauswahl. Jedes Produkt wird in Hashentic zu einer Produktlinie; Ihr Tarif begrenzt, wie viele Sie schützen können. Lange Listen werden auf Seiten aufgeteilt und erhalten ein Suchfeld.
2. Öffnen Sie **Codes**, wählen Sie das Produkt (und eine Variante, wenn Sie mehrere verkaufen), geben Sie die **Anzahl der Codes** ein und klicken Sie auf **Codes ausstellen**. Vor dem Ausgeben bittet die App um Bestätigung: Der Dialog zeigt, wie viele Codes Sie ausgeben und wie viele QR-Codes in diesem Monat noch übrig sind.
3. Sobald die Charge *Fertig* zeigt, klicken Sie auf **PDF-Etiketten herunterladen** für druckfertige A4-Bögen oder auf **CSV herunterladen** für Ihren Etikettendrucker. Ein großes PDF zeigt während der Erstellung seinen Fortschritt; **Abbrechen** bricht sie ab.

Die Seite **Codes** listet Ihre Chargen mit 25 pro Seite auf, die neuesten zuerst; blättern Sie mit den Seitensteuerungen unter der Tabelle. Die Spalte **Quelle** zeigt **Bestellung** für automatisch zu einer Bestellung ausgegebene Codes und **Manueller Stapel** für Chargen, die Sie selbst ausgegeben haben.

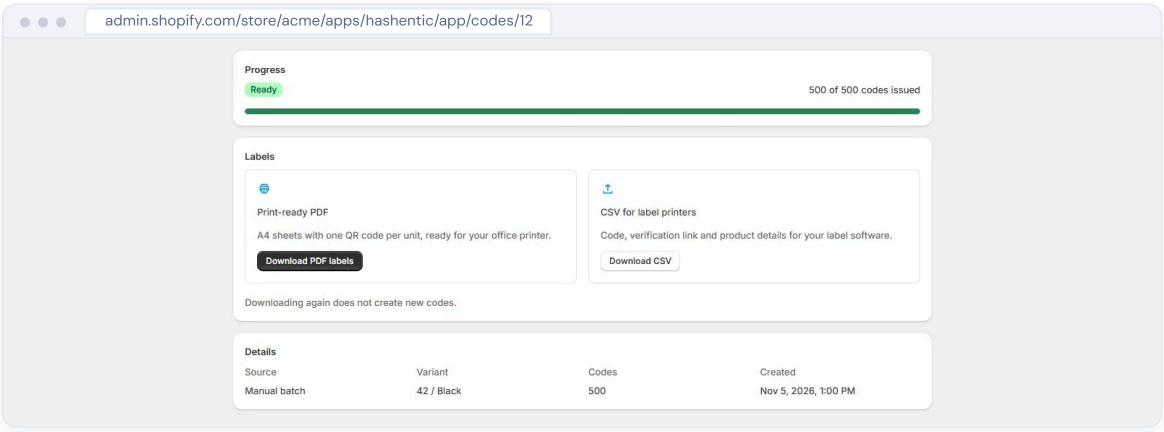
Jeder Code behält den Produkttitel und die Variante, für die er ausgegeben wurde. Wenn Sie das Produkt in Shopify ändern oder löschen, bleibt ein gedruckter Code trotzdem prüfbar. **Schutz beenden** fragt nach einer Bestätigung: Das Produkt erhält dann keine neuen Codes, und bereits dafür ausgegebene Codes bleiben prüfbar.



Geschützte Produkte. Aus Shopify gewählte Produkte werden zu Produktlinien.



Codes. Charge ausgeben und Fortschritt verfolgen; der Balken zeigt das QR-Kontingent des Monats.



Charge. Etiketten als PDF oder CSV herunterladen, sobald alle Codes ausgegeben sind.

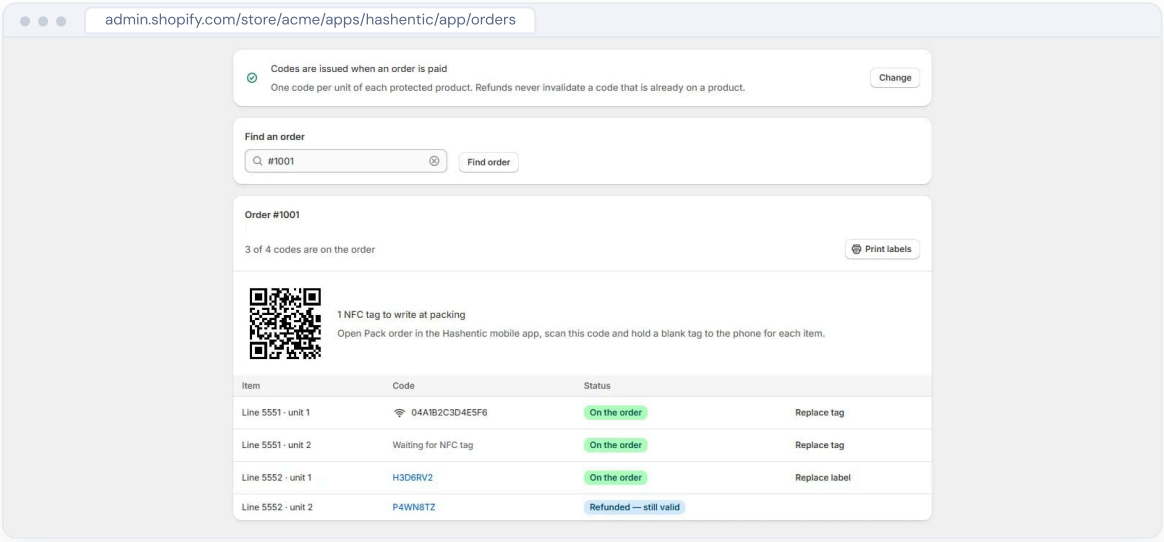
> **Wer Codes ausgeben darf**
>
> Das Ausgeben von Codes verbraucht Ihr monatliches QR-Kontingent und bezahlte Pakete. Deshalb kann standardmäßig nur der Shopinhaber Codes ausgeben, drucken und exportieren. Der Inhaber kann das unter **Einstellungen** ändern. Dieselbe Regel gilt für **Produkte schützen**, **Schutz beenden** und das Ändern von **Bestellungen erhalten**: Mitarbeiter sehen diese Bedienelemente deaktiviert.

Codes für jede Bestellung

Wählen Sie unter **Einstellungen** bei **Codes automatisch ausstellen**: **Wenn eine Bestellung bezahlt ist** (Standard), **Wenn eine Bestellung ausgeführt ist** oder **Aus — ich stelle Stapel selbst aus**. Hashentic gibt dann für jede Einheit jedes geschützten Produkts der Bestellung einen Code aus.

- Öffnen Sie **Bestellungen** und geben Sie die Bestellnummer ein, um ihre Codes zu sehen und Etiketten dafür zu drucken. Jede Einheit zeigt ihr Produkt und ihre Variante, ebenso ihr Etikett, sodass Etiketten verschiedener Produkte einer Bestellung nicht verwechselt werden können. Die Bestellnummer steht in der Adresse der Seite, sodass die Suche ein Neuladen und die Zurück-Taste des Browsers übersteht.
- Klicken Sie bei einem beschädigten Etikett auf **Etikett ersetzen** und bestätigen Sie. Der Ersatz erhält einen neuen Code und verbraucht einen QR-Code Ihres monatlichen Kontingents; der alte bleibt prüfbar. Ersetzen ist möglich, sobald eine Einheit ihren Code hat.
- Zum Nachschlagen einer Bestellung ist Zugriff auf Bestellungen in Shopify nötig: Mitarbeiter ohne diesen Zugriff sehen statt der Bestellung einen Hinweis.
- Wird eine Bestellung bearbeitet, kommen für hinzugefügte Einheiten Codes hinzu; entfernte Einheiten werden als freigegeben markiert.
- Stornierte und erstattete Einheiten werden in der Liste markiert, ihre Codes werden aber nie abgeschaltet: Ein echtes Produkt bleibt auch nach einer Erstattung echt.
- Hashentic liest nur Bestellpositionen, Produkte, Varianten und Mengen. Namen, E-Mail-Adressen oder Anschriften von Kunden werden nie gespeichert.

Einstellungen nutzt die Speicherleiste von Shopify: Sobald Sie etwas ändern, erscheinen **Speichern** und **Verwerfen**, und Shopify warnt Sie, wenn Sie die Seite mit ungespeicherten Änderungen verlassen.

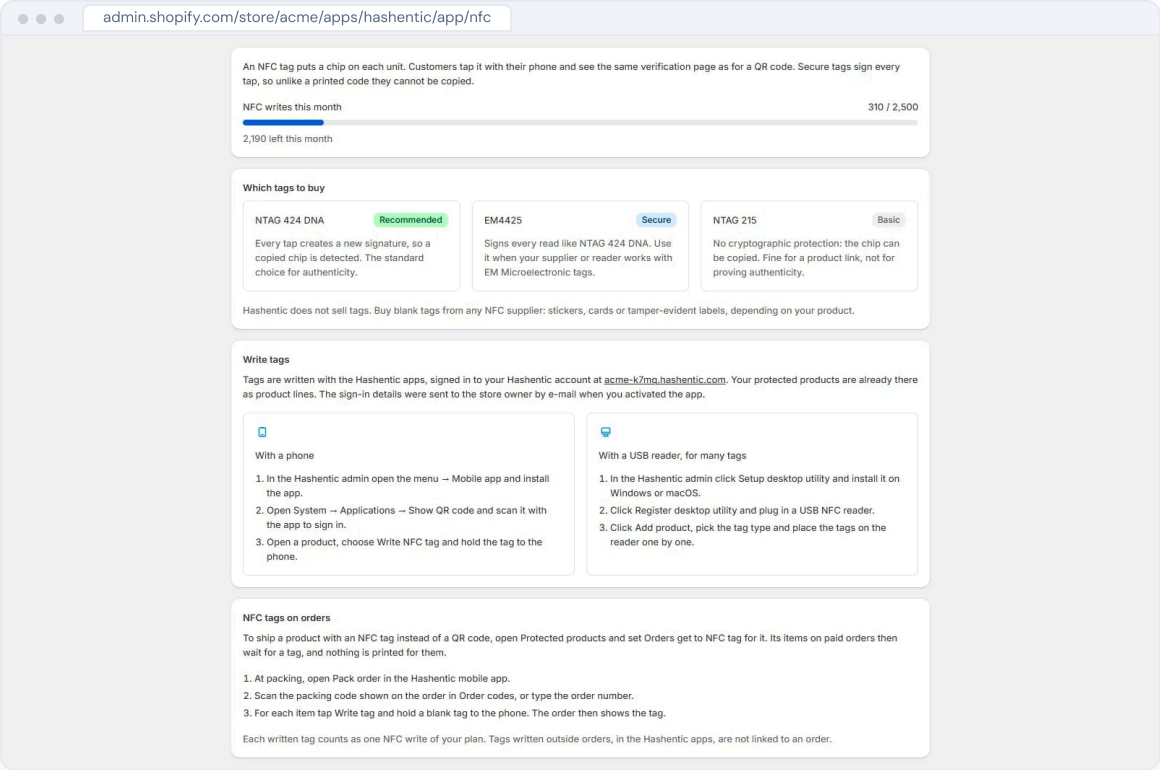


Bestellungen. Ein Code pro Einheit; eine erstattete Einheit behält ihren gültigen Code.

NFC-Tags

Öffnen Sie **NFC-Tags** in der App. Dort sehen Sie, wie viele Tags Sie diesen Monat schreiben können, welche Tags Sie kaufen sollten und wie Sie sie schreiben. Empfohlen ist NTAG 424 DNA: Jedes Antippen wird signiert, ein kopierter Chip fällt auf. NTAG 215 hat keinen Kopierschutz.

Tags werden mit der Hashentic-Mobile-App oder mit dem Desktop-Programm und einem USB-Lesegerät geschrieben, angemeldet bei Ihrem Hashentic-Konto. Ihre geschützten Produkte sind dort bereits als Produktlinien vorhanden. So geschriebene Tags sind keiner Bestellung zugeordnet.



NFC-Tags. Welche Tags Sie kaufen und wie Sie sie schreiben.

NFC-Tags für Bestellungen

Um ein Produkt mit NFC-Tag statt QR-Code zu versenden, öffnen Sie **Geschützte Produkte** und stellen Sie **Bestellungen erhalten** für dieses Produkt auf **NFC-Tag**. Die Spalte **Bestellungen erhalten** erscheint, wenn Ihr Tarif NFC-Schreibvorgänge enthält. Seine Einheiten in neuen Bestellungen erhalten dann keinen QR-Code und warten auf ein Tag; andere Produkte derselben Bestellung behalten ihre QR-Codes. Auch bei **Wenn eine Bestellung ausgeführt ist** erscheinen die Einheiten von NFC-Produkten schon, sobald die Bestellung bezahlt ist, damit Sie sie beim Verpacken taggen können; QR-Codes warten weiterhin auf die Ausführung.

1. Öffnen Sie die Bestellung unter **Bestellungen**. Einheiten von NFC-Produkten zeigen *Wartet auf NFC-Tag*, und die Bestellung zeigt einen Packcode.
2. Öffnen Sie beim Verpacken **Pack order** in der Hashentic-Mobile-App und scannen Sie den Packcode oder geben Sie die Bestellnummer ein.
3. Tippen Sie für jede Einheit auf **Write tag** und halten Sie ein leeres Tag an das Telefon. Die Bestellung unter **Bestellungen** zeigt danach das Tag.

Jedes geschriebene Tag zählt als ein NFC-Schreibvorgang Ihres Tarifs; wartende Einheiten verbrauchen keine QR-Codes. Nur Mitarbeiter, die Produkte schreiben dürfen und Zugriff auf die Produktlinie haben, sehen die Bestellung in der Mobile-App. Einheiten, die bereits in einer Bestellung sind, behalten ihren Typ, wenn Sie das Produkt wieder auf QR-Code umstellen.

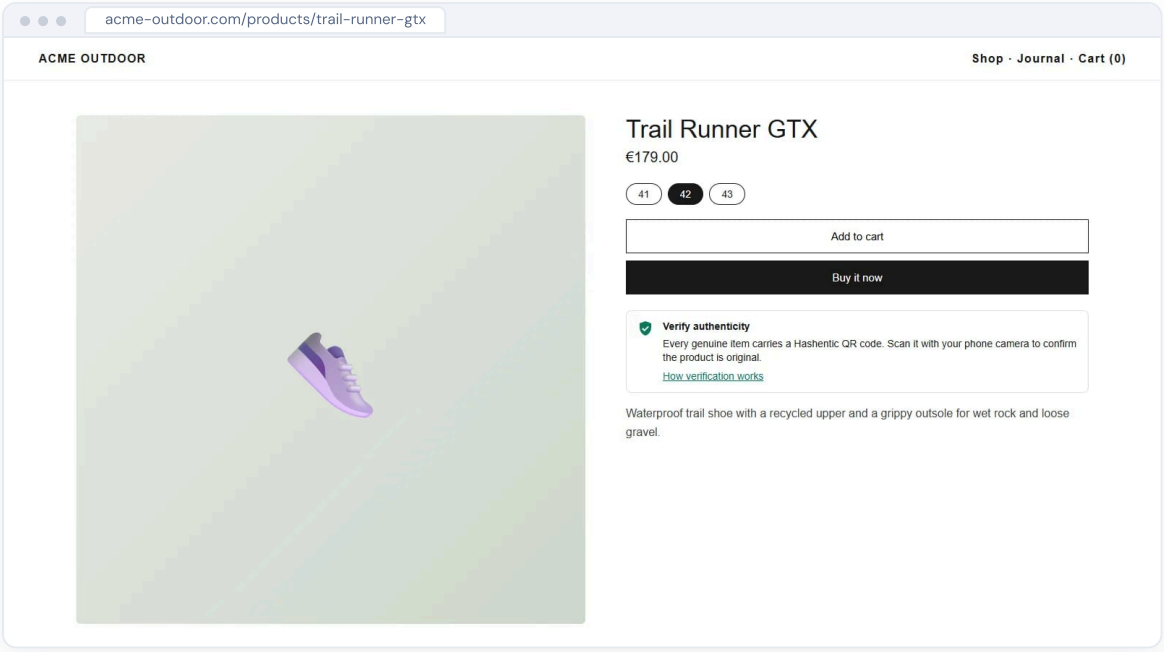
„Echtheit prüfen“ im Shop anzeigen

Am schnellsten geht es mit **Theme-Editor öffnen** auf der Startseite der App: Die Produktvorlage öffnet sich mit dem Block, der nur noch hinzugefügt werden muss. Sie können ihn auch von Hand hinzufügen:

1. Öffnen Sie in Shopify **Onlineshop** → **Themes** → **Anpassen** und wechseln Sie zu einer Produktseite.
2. Klicken Sie auf **Block hinzufügen**, wählen Sie unter **Apps** den Block **Echtheit prüfen** und platzieren Sie ihn nahe dem Kaufen-Button.
3. Legen Sie fest, ob der Block **Nur geschützte Produkte** oder **Alle Produkte** zeigt, und speichern Sie.

Der Block verlinkt Ihre Prüfseite und erklärt Kunden, wie sie ein Produkt prüfen. Er ist auf Englisch, Deutsch, Spanisch, Französisch, Polnisch, Portugiesisch, Russisch und Chinesisch übersetzt und erzeugt beim Laden der Seite keine zusätzlichen Anfragen.

Im Theme-Editor wird der Block immer angezeigt, mit einem Vorschauhinweis, wenn Kunden ihn nicht sehen würden (das Produkt ist nicht geschützt oder Hashentic ist noch nicht aktiviert). Der Hinweis erscheint nie in Ihrem Live-Shop. Der Blocktext sagt, dass jeder echte Artikel einen Hashentic-QR-Code oder NFC-Tag trägt.

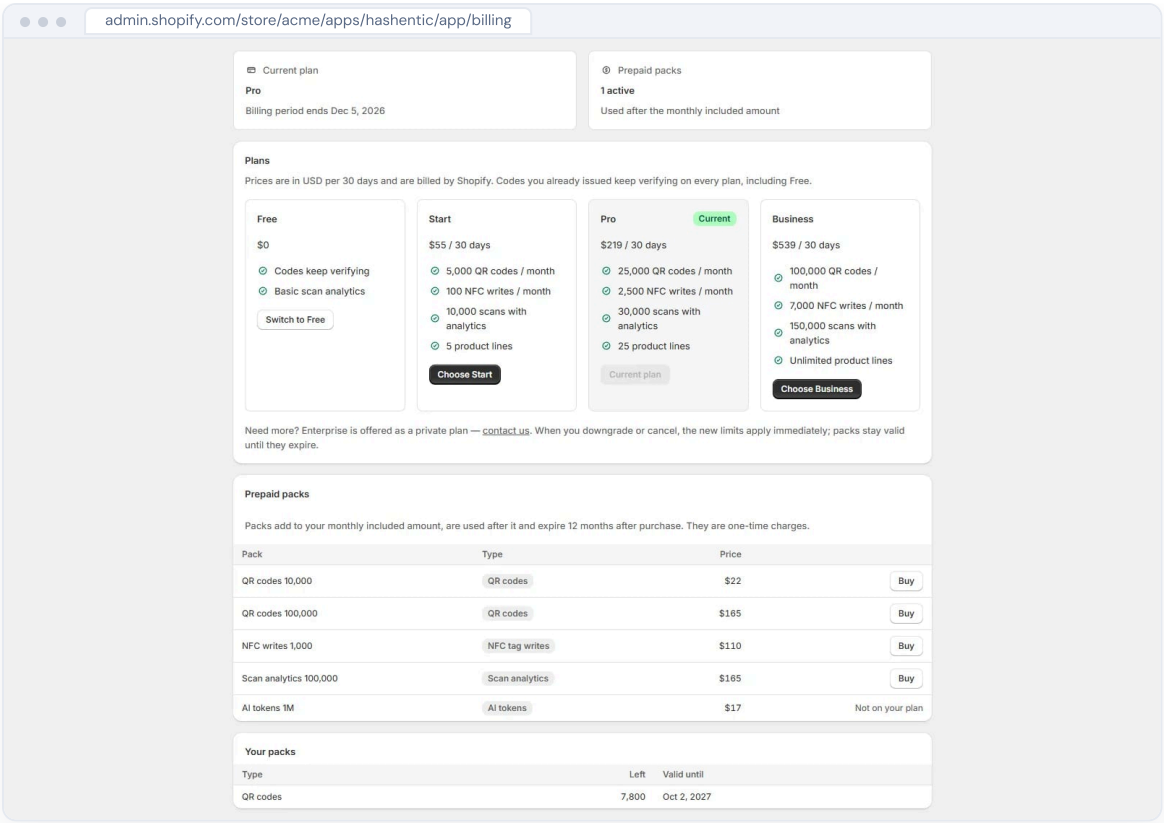


Block **Echtheit prüfen** auf einer Produktseite.

Tarife und Pakete

Öffnen Sie **Tarif und Pakete**. Tarife werden von Shopify alle 30 Tage in US-Dollar mit Ihrer Shopify-Rechnung abgerechnet; Enterprise gibt es auf Anfrage als privaten Tarif. Prepaid-Pakete (QR-Codes, NFC-Schreibvorgänge, Scan-Analysen, Workflow-Ausführungen, KI) sind Einmalzahlungen, werden nach dem monatlich enthaltenen Umfang verbraucht und laufen 12 Monate nach dem Kauf ab. Pakete setzen einen kostenpflichtigen Tarif voraus, der diesen Pakettyp enthält; während der Testphase zeigen solche Pakete **Erfordert einen kostenpflichtigen Tarif**. Nur der Shopinhaber kann den Tarif ändern oder Pakete kaufen.

Die Wahl eines Tarifs und **Zum Tarif Kostenlos wechseln** verlangen zuerst eine Bestätigung. Wählen Sie während der Testphase einen Tarif, endet die Testphase: Die Abrechnung beginnt an dem Tag, an dem Sie die Belastung in Shopify genehmigen, und die Grenzen des Tarifs ersetzen die der Testphase. Bei einem Downgrade gelten die neuen Grenzen sofort; Scans bestehender Codes funktionieren immer weiter.



Tarif und Pakete. Tarife und Einmalpakete, abgerechnet über Shopify.

Deinstallieren

Wenn Sie die App deinstallieren, endet das Shopify-Abonnement, Ihr Hashentic-Konto wechselt in den Free-Tarif und die Verbindung zu Shopify wird getrennt. Ihre Prüfseite und alle gedruckten Codes funktionieren weiter. 48 Stunden später bittet Shopify uns, die Shopdaten zu löschen: Wir entfernen alle Shopify-IDs und Verknüpfungen, und das Konto bleibt Ihnen als normales Hashentic-Konto erhalten. Installieren Sie innerhalb dieser 48 Stunden erneut, verbindet sich die App wieder mit demselben Konto; danach legt eine neue Installation ein neues Konto an. In beiden Fällen aktivieren Sie erneut und wählen erneut einen Tarif.

Fragt ein Kunde nach der Deinstallation bei Ihrem Shop nach seinen Daten, leitet Shopify die Anfrage an uns weiter und wir senden dem Shopinhaber per E-Mail die Codes, die mit den Bestellungen dieses Kunden verknüpft sind, damit Sie dem Kunden antworten können. Nachdem die Shopdaten gelöscht sind (48 Stunden nach der Deinstallation), speichern wir zu diesen Bestellungen nichts mehr; kann die E-Mail nicht zugestellt werden, antwortet Ihnen unser Support.

Nachschlagewerk

Listen zum Nachschlagen: Gründe fehlgeschlagener Scans, Inhalte für Seitenvorlagen, Sprachen und Limits sowie Antworten auf häufige Fragen.

A Gründe fehlgeschlagener Verifizierungen

B Platzhalter in Vorlagen

C Sprachen, Formate und Limits

D Fehlerbehebung und häufige Fragen

ANHANG

A Gründe fehlgeschlagener Verifizierungen

Die Anzeige unter *Reason* im Tab Invalid von Verifications und ihre übliche Bedeutung.

Grund	Wann er auftritt	Übliche Bedeutung
Invalid product	Code oder Link unbekannt, Produkt gelöscht oder NFC-Tag nicht fertig beschrieben.	Gefälschter oder falsch eingegebener Code
Invalid PICC	NTAG 424: Verschlüsselte Tag-Daten lassen sich nicht zum erwarteten Tag entschlüsseln.	Gefälschter oder geklonter Tag
Invalid CMAC	NTAG 424: Die kryptografische Signatur des Tags ist falsch.	Manipulierter oder kopierter Link
Invalid signature	EM4425: Signierte Daten sind fehlerhaft aufgebaut oder die Signatur ist falsch.	Gefälschter Tag
Invalid UID	Die eindeutige Tag-ID entspricht nicht der für das Produkt registrierten.	Vertauschter oder gefälschter Tag
Invalid transaction	Die Transaktion des Links entspricht nicht dem Integritätsnachweis des Produkts.	Manipulierter Link
Already verified	Der Einmalcode eines sicheren Tags wurde bereits verwendet: derselbe Link wurde erneut geöffnet.	Weitergegebener Link oder Wiederholung
Read counter mismatch	Der Tag-Zähler ist gegenüber früheren Scans zurückgegangen.	Geklonter Tag
Product is blocked	Ihr Team oder ein Workflow hat das Produkt gesperrt.	Gestohlener, zurückgerufener oder verdächtiger Artikel
This authentication has been blocked	Dieser bestimmte Tag oder Code wurde gesperrt.	Bekannte Tag-Kopie
This product is only available for internal verification	Die Produktlinie ist auf interne Prüfungen beschränkt.	Nicht für öffentliche Scans
Unspecified	Unerwarteter Fehler während der Prüfung.	Bei häufigem Auftreten Support kontaktieren

Gründe in Fehlerseitenregeln

Fehlerseitenregeln gruppieren Gründe, sodass eine Regel verwandte Fehler abdeckt:

Regelbedingung	Gründe
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	Jeder andere Grund in der obigen Tabelle

Barcodes und NTAG 215

Diese enthalten einen festen Link und erkennen selbst keine Kopien: Jeder Scan eines kopierten QR-Codes ist gültig. Überwachen Sie sie mit den Betrugssignalen *Velocity spike* und *Gray market* und sperren Sie Codes, die eindeutig kopiert werden.

ANHANG

B Platzhalter in Vorlagen

In Blockeditor- und eigenen HTML-Vorlagen werden Wörter in eckigen Klammern beim Anzeigen durch echte Werte ersetzt. Groß- und Kleinschreibung spielt keine Rolle; unbekannte Platzhalter bleiben unverändert.

Platzhalter	Ersetzt durch
[AssetName]	Name des Assets
[AssetDescription]	Beschreibung des Assets
[VerifiedAt]	Datum und Uhrzeit der Verifizierung (UTC)
[VerifiedDate]	Datum der Verifizierung
[VerificationMethod]	Typ des gescannten Datenträgers
[*propertyName*]	Produktwert eines beliebigen Asset-Feldes, etwa **[serialNumber]**, **[caseMaterial]**
GS1-Felder	Für GS1-Assets: **[gtin]**, **[brandName]**, **[tradeItemDescription]**, **[netContent]**, **[batchLotNumber]**, **[expiryDate]** und weitere GS1-Attribute
Passdaten	Jedes Element der obersten Ebene des Produktpasses des Assets, anhand seines Schlüssels
[TransactionId] · **[TransactionLink]**	Integritätsnachweis und Explorer-Link bei Blockchain-Speicherung der Assets
[ErrorMessage]	Nur auf der Seite für ungültige Scans: Grund des Fehlschlags
[FailReason]	Nur auf der Seite für ungültige Scans: Fehlergruppe als Code, `already-scanned`, `blocked`, `internal-only` oder `auth-failed`, etwa zum Wechseln von Texten in eigenem HTML

Verborgene Felder

Ein Platzhalter setzt den Wert auch ein, wenn das Feld als *Hidden* markiert ist. Verwenden Sie nur Felder auf einer Seite, die Kunden sehen dürfen.

Integration guide im Administrationsbereich (*Custom HTML templates*) erklärt, wie eigene HTML-Seiten die vollständigen Verifizierungsdaten per Skript auslesen und wie eine externe Website sie empfängt.

ANHANG

C Sprachen, Formate und Limits

Element	Wert
Sprachen des Administrationsbereichs	English, Deutsch, Español, Français, Polski, Português, Русский, 中文
Assistent, Dokumente und Formulare der Verifizierungsseite	Dieselben acht Sprachen gemäß Besucherbrowser; KI-Antworten folgen der Sprache der Frage
Sprachen von Seitenvorlagen	Basisinhalt plus bis zu 10 Sprachen pro Vorlage; die Browsersprache entscheidet
Integrierte Verifizierungsseite	Die acht Sprachen des Administrationsbereichs gemäß Besucherbrowser
Sprachen der mobilen App	Englisch, Französisch, Portugiesisch und Russisch gemäß Telefon
NFC-Tags	NTAG 424 DNA, NTAG 215, EM4425
Barcodes	QR-Code, DataMatrix, Code 128; GS1 Digital Link und GS1-Elementstrings für GS1-Assets
Feldtypen	Text, Email, Number, Select, Lookup, Date, Checkbox
Importdateien	CSV (Komma, Semikolon, Tabulator oder senkrechter Strich), XLSX, XLS; bis 100.000 Zeilen und 10 MB
Generate by number	Bis 50.000 Produkte gleichzeitig
Barcode-Massenoperationen	Bis 200.000 Datensätze; Massenaktualisierungen bis 50.000 Einträge
ERP-Abruf	Vorschau mit 50 Datensätzen; Abruf bis 100.000
Dokumente	PDF, DOCX, TXT, Markdown; standardmäßig je 10 MB (bis 25); bis 20 pro Produkt, 50 pro Asset, 100 markenweit
Labels	Bis 15 pro Asset
Passwörter	12–128 Zeichen mit mindestens einem Buchstaben und einer Ziffer; 5 Fehlanmeldungen sperren das Konto für 5 Minuten
Wiederherstellungscodes	10 einmalig verwendbare Codes pro Benutzer
Desktop-Dienstprogramm	Windows x64; macOS Apple Silicon und Intel; USB-NFC-Lesegeräte
Mobile App	Android 8.0+; iPhone mit iOS 16.4+; NFC-fähiges Telefon für Tags

Ihre Lizenz setzt zusätzliche Limits: Benutzer, Assets, Tags, Barcodes, Produkte, KI-Nutzung, Dokumentenspeicher, Workflow-Durchläufe und Kundenfragen. Scan-Analysen, neue QR-Codes und NFC-Schreibvorgänge haben Monatslimits, die am 1. jedes Monats (UTC) zurückgesetzt werden; Prepaid-Pakete gelten 12 Monate und werden erst nach der im Monat enthaltenen Menge verbraucht. Ihre aktuelle Nutzung sehen Sie unter System → License, die Tarife unter Lizenz.

ANHANG

D Fehlerbehebung und häufige Fragen

Ein Menüpunkt aus diesem Handbuch fehlt.

Er benötigt eine Berechtigung, die Sie nicht besitzen, oder eine Funktion außerhalb Ihrer Lizenz. Fragen Sie Ihre Administration nach den Berechtigungen und Lizenzfunktionen Ihres Kontos.

"Write" bleibt unter Add new deaktiviert.

Bewegen Sie den Mauszeiger darüber, um den Grund zu sehen: kein Asset ausgewählt, Desktop-Dienstprogramm oder Lesegerät nicht verbunden, kein Tag auf dem Leser, Tag-Typ nicht lizenziert oder Tag-/Barcode-Limit erreicht (siehe Schreiben gestoppt: Monatslimit erreicht). Leere Pflichtfelder werden beim Klicken auf Write gemeldet.

Die obere Schaltfläche zeigt "Connect application", obwohl das Dienstprogramm läuft.

Das Dienstprogramm ist mit einem anderen Konto oder von einem anderen Computer aus angemeldet. Registrieren Sie es erneut unter Setup desktop utility oder erzeugen Sie den Desktop application token neu und fügen Sie ihn ein.

"Reader is not responding" oder "The NFC reader stopped responding".

Das Lesegerät hat dem Desktop-Dienstprogramm 15 Sekunden lang nicht geantwortet, meist beim Beschreiben oder Formatieren eines Tags. Der Status in der Kopfzeile wird orange, und das Schreiben ist gesperrt, bis das Lesegerät wieder antwortet. Ziehen Sie das Lesegerät ab, schließen Sie es wieder an und beschreiben Sie den Tag erneut. Bleibt die Meldung, starten Sie das Desktop-Dienstprogramm neu.

Schreiben gestoppt: Monatslimit erreicht.

Monthly NFC tag limit reached oder *Monthly QR code limit reached* bedeutet, dass die NFC-Schreibvorgänge oder neuen QR-Codes dieses Monats einschließlich der Pakete aufgebraucht sind. Administrationsbereich, mobile App und Desktop-Dienstprogramm zeigen dieselbe Meldung. Das Limit wird am 1. des Monats (UTC) zurückgesetzt. Um sofort weiterzumachen, kann Ihre Administration zu einem höheren Tarif wechseln oder, wenn der Tarif dieses Paket anbietet, über **Order a pack** auf der Lizenzseite eines bestellen und die Rechnung bezahlen (nicht auf Free oder in der Testphase); das Schreiben funktioniert dann nach etwa 5 Minuten wieder. Siehe Monatslimits und Pakete.

Manche Scans haben keinen Standort und kein Gerät.

Ist das Kontingent **Scan analytics** dieses Monats aufgebraucht, pausieren Standort- und Geräteanalysen, bis Sie ein Paket kaufen oder der nächste Monat beginnt. Die Scans werden weiterhin verifiziert und erfasst. Scans aus privaten Netzwerken oder ohne die Lizenzfunktion Geolocation analytics erhalten nie ein Land.

Ein Kunde meldet, dass ein echtes Produkt "not verified" zeigt.

Suchen Sie das Produkt unter Verifications → Invalid. "Already verified" bedeutet, dass ein alter Tag-Link erneut geöffnet wurde: Der Kunde sollte den Tag erneut antippen, oder Sie aktivieren *Allow already verified asset page*. "Product is blocked" bedeutet, dass jemand es gesperrt hat.

Ein Kunde sieht die Verifizierungsseite in der falschen Sprache.

Die Seite folgt der Browsersprache des Besuchers. Fehlt eine Vorlagenversion in dieser Sprache, erscheint der Basisinhalt. Ergänzen Sie die Sprache an der Vorlage (Die Verifizierungsseite übersetzen).

Das Dashboard wirkt leer.

Prüfen Sie Asset-Auswahl und Zeitraum (D, W, M, Y, All). Neue Scans erscheinen unter Umständen erst nach etwa einer Minute in Diagrammen.

Warum haben manche Scans kein Land?

Der Standort wird aus der Internetadresse des scannenden Geräts ermittelt und benötigt die Lizenzfunktion Geolocation analytics. Scans aus privaten Netzwerken können nicht lokalisiert werden.

Kann ich ein Feld ändern, wenn bereits Produkte bestehen?

Sie können Felder bearbeiten und ergänzen, aber weder löschen noch ihren Eigenschaftsnamen ändern. Werte bestehender Produkte lassen sich nur bei Feldern der Stufe Update ändern.

Ein Dokument bleibt bei "Waiting for indexing" oder zeigt "Indexing failed".

Die Indexierung läuft im Hintergrund und kann einige Minuten dauern. Gescannte PDFs ohne Textebene sind nicht lesbar: Laden Sie eine textbasierte PDF hoch und verwenden Sie Re-index.

Workflows mit HTTP request lassen sich nicht speichern.

Ergänzen Sie zuerst das Adressmuster (zum Beispiel `https://crm.example.com/*`) unter Settings → Workflows URL allowlist.

Wie gebe ich einem Auditor schreibgeschützten Zugriff?

Erstellen Sie ein Konto mit der Rolle Benutzer, nur mit Leseberechtigungen (Produkte, Verifizierungen, Assets) und den entsprechenden erlaubten Assets. Änderungen werden im Audit-Protokoll erfasst.

Wo finden Entwickler Informationen zu API und Webhooks?

Öffnen Sie **Integration guide** unten im Menü: Anleitungen für eigene HTML-Vorlagen, Workflows, REST API, Webhooks und ERP-Integration.