gründerkind

BENUTZERHANDBUCH

SHOPWARE 6 · SPAM-SCHUTZ

Turnstile Ultimate.

Cloudflare Turnstile für Newsletter, Registrierung, Gastkauf, Kontakt und Widerruf – ohne Bilderrätsel, ohne Abtippen, auch über die Store-API.

- Formulare
- Store-API
- Ausfallsicher
- Pro Verkaufskanal

Version 1.1.0

Für Shopware 6.7 · Stand November 2026

Gründerkind GmbH
BmaniaTurnstileUltimate
dev@gruenderkind.com

Inhalt

Vom Cloudflare-Konto über die Einstellungen bis zur Kontrollrunde – alles, was Sie für einen spamfreien Shop brauchen.

1 Einleitung 3

2 In fünf Minuten startklar 4

3 Cloudflare einrichten 5

4 So schützt das Plugin Ihre Formulare 6

5 Aktivierung und geschützte Formulare 7

6 Schlüssel und Darstellung 8

7 Prüfung auf dem Server 9

8 Store-API und Headless 10

9 Betrieb: Cache, Log, Updates 11

10 Ihre Prüfpflicht: das Ergebnis kontrollieren 12

11 Häufige Fragen 13

1 Einleitung

Welches Problem das Plugin löst, wo seine Grenzen liegen und was Sie brauchen.

Wofür Sie dieses Plugin brauchen

Bots melden fremde E-Mail-Adressen für Ihren Newsletter an, legen Fake-Konten an und füllen Kontaktformulare mit Spam. Jede falsche Newsletter-Anmeldung löst eine Bestätigungsmail an eine fremde Adresse aus – das schadet dem Ruf Ihres Mailversands. Der Honeypot von Shopware hält nur einen Teil der Bots ab, und klassische Captchas mit Bilderrätseln vergraulen echte Kunden.

Turnstile Ultimate bindet **Cloudflare Turnstile** in alle Shopware-Formulare ein, die ein Captcha vorsehen. Die Prüfung läuft im Hintergrund; nur wenn Cloudflare unsicher ist, klickt der Besucher einmal einen Haken an. Zusätzlich verlangt das Plugin das Prüfzeichen auch bei direkten Aufrufen der Store-API – dem Weg, auf dem Bots Formulare gern umgehen.

> **SCHUTZ JA, GARANTIE NEIN**
>
> Turnstile senkt Spam erheblich, kann aber nicht jeden Missbrauch durch echte Menschen verhindern. Das Plugin ist ein Werkzeug, **keine Rechtsberatung**: Datenschutzerklärung und rechtliche Bewertung bleiben beim Shopbetreiber (Kapitel 10).

Systemanforderungen

Voraussetzung	Wert
Shopware	6.7.0 oder neuer (Eintrag im Cookie-Manager ab 6.7.3)
PHP	8.2 oder neuer
Cloudflare	kostenloses Konto mit einem Turnstile-Widget; Ihre Domain muss nicht über Cloudflare laufen
Theme	beliebig; Formulare müssen das Shopware-Captcha-Template einbinden

2 In fünf Minuten startklar

Der kürzeste Weg zum ersten geschützten Formular.

Installation

```
bin/console plugin:refresh
bin/console plugin:install --activate BmaniaTurnstileUltimate
bin/console theme:compile
bin/console cache:clear
```

Alternativ im Administrationsbereich unter **Erweiterungen › Meine Erweiterungen** installieren und aktivieren und danach das Theme neu zuweisen.

Die ersten Schritte

1. **Widget bei Cloudflare anlegen.** Site Key und Secret Key notieren (Kapitel 3).
2. **Schlüssel eintragen.** Unter **Erweiterungen › Meine Erweiterungen › Turnstile Ultimate › Konfigurieren** beide Schlüssel in der Karte „Cloudflare-Schlüssel“ speichern.
3. **Schutz einschalten.** „Formulare mit Cloudflare Turnstile schützen“ aktivieren – global oder zuerst nur für einen Verkaufskanal.
4. **Formulare wählen.** Unter „Geschützte Formulare“ festlegen, was geprüft wird (Kapitel 5).
5. **Kontrollrunde gehen.** Jedes geschützte Formular einmal absenden (Kapitel 10).

> **WENN KEIN WIDGET ERSCHEINT**
>
> Prüfen Sie in dieser Reihenfolge: Ist der Hauptschalter im richtigen Verkaufskanal an? Sind **beide** Schlüssel eingetragen? Wurde das Theme nach der Installation neu kompiliert? Ist das Formular unter „Geschützte Formulare“ eingeschaltet? Im Modus „Nur wenn ein Klick nötig ist“ ist das Widget für die meisten Besucher bewusst unsichtbar.

3 Cloudflare einrichten

Ein Widget, alle Domains, zwei Schlüssel – mehr braucht es nicht.

Widget anlegen

1. **Konto öffnen.** Im Cloudflare-Dashboard den Bereich **Turnstile** aufrufen; ein kostenloses Konto genügt.
2. **Widget hinzufügen.** Einen Namen vergeben und als Modus **Managed** wählen.
3. **Domains eintragen.** Jede Shop-Domain mit und ohne **www**, also z. B. **meinshop.de** und **www.meinshop.de**.
4. **Schlüssel übernehmen.** Site Key und Secret Key in die Plugin-Konfiguration kopieren.

> **FEHLENDE DOMAIN HEISST: FORMULAR SCHEITERT**
>
> Steht eine Domain nicht im Widget, liefert Cloudflare dort kein gültiges Prüfzeichen und **jede Absendung wird abgewiesen**. Nach dem Hinzufügen eines neuen Verkaufskanals deshalb immer die Domains im Widget ergänzen.

Testschlüssel

Zum Ausprobieren ohne echtes Widget stellt Cloudflare feste Testschlüssel bereit. Die Domainprüfung (Kapitel 7) muss dabei aus bleiben.

Verhalten	Site Key	Secret Key
besteht immer	1x00000000000000000000AA	1x0000000000000000000000000000000AA
scheitert immer	2x00000000000000000000AB	2x0000000000000000000000000000000AA
erzwingt Klick	3x00000000000000000000FF	–

4 So schützt das Plugin Ihre Formulare

Was zwischen dem ersten Klick ins Formular und dem gespeicherten Eintrag passiert.

Der Ablauf

1. **Besucher nutzt das Formular.** Erst wenn er hineinklickt oder absendet, lädt das Cloudflare-Skript – vorher wird Cloudflare nicht kontaktiert.
2. **Turnstile prüft im Hintergrund.** Das Ergebnis ist ein Prüfzeichen (Token), das mit dem Formular mitgeschickt wird.
3. **Ihr Server fragt nach.** Vor dem Speichern prüft Shopware das Token direkt bei Cloudflare.
4. **Ergebnis.** Gültig: Das Formular wird wie gewohnt verarbeitet. Fehlt das Token oder ist es ungültig: Das Formular erscheint mit Hinweis wieder, die Eingaben bleiben erhalten.

Gut zu wissen

- **Ein Token gilt genau einmal.** Nach jeder Antwort bei Ajax-Formularen (Newsletter, Kontakt) steht automatisch eine neue Prüfung bereit.
- **Kein vorschnelles Absenden.** Klickt jemand, bevor die Prüfung fertig ist, hält das Plugin den Versand kurz an und schickt das Formular danach selbst ab.
- **Mehrere Formulare je Seite.** Jedes bekommt sein eigenes Widget; das Skript lädt trotzdem nur einmal.
- **Honeypot bleibt.** Der Shopware-Honeypot unter **Einstellungen › Grundeinstellungen › Captcha** wirkt zusätzlich. Turnstile selbst erscheint dort nicht, sondern wird im Plugin eingeschaltet.

> **GLOBAL ODER PRO VERKAUFSKANAL**
>
> Alle Einstellungen lassen sich unter „Alle Verkaufskanäle“ setzen und je Kanal überschreiben. So können Sie **Kanal für Kanal einschalten** – etwa zuerst im Shop mit dem meisten Spam – und Schlüssel einmal global hinterlegen.

5 Aktivierung und geschützte Formulare

Welche Schalter es gibt und welches Formular welcher Schalter steuert.

Karte „Aktivierung“

Feld	Bedeutung	Standard
Formulare mit Cloudflare Turnstile schützen	Hauptschalter je Verkaufskanal. Aus: kein Widget, kein Skript, keine Prüfung.	aus
Auch die Store-API schützen	Verlangt das Token auch bei direkten Store-API-Aufrufen der unten gewählten Formulare (Kapitel 8).	an

Karte „Geschützte Formulare“

Feld	Wirkt auf	Standard
Newsletter-Anmeldung	Newsletter-Erlebniswelten und Newsletter-Formulare des Themes, die das Captcha einbinden	an
Registrierung und Gastkauf	Kundenregistrierung und Gastbestellung – Shopware nutzt dafür dasselbe Formular	an
Kontaktformular	Kontaktformulare in Erlebniswelten, auch im Modal	an
Widerrufsformular	Online-Widerrufsformular (nur in Shopware-Versionen, die es haben)	an
Gastbestellung in Kundenkonto umwandeln	Konto-Umwandlung nach einer Gastbestellung (nur, wo vorhanden)	an
Anmeldung (Login)	Login-Formular; einschalten, wenn Bots Passwörter durchprobieren	aus

AUSGESCHALTET HEISST WIRKLICH AUS

Ein abgeschaltetes Formular zeigt kein Widget, lädt nichts von Cloudflare und wird **weder in der Storefront noch über die Store-API** geprüft. Captcha-Formulare anderer Erweiterungen, die keinem Schalter zugeordnet sind, bleiben geschützt, solange der Hauptschalter an ist.

6 Schlüssel und Darstellung

Wie das Widget aussieht – und wann Ihre Kunden es überhaupt sehen.

Karte „Cloudflare-Schlüssel“

Feld	Bedeutung	Standard
Site Key	Öffentlicher Schlüssel des Widgets; wird an die Storefront ausgegeben.	leer
Secret Key	Geheimer Schlüssel für die Prüfung auf dem Server. Er erscheint nie in der Storefront und nie im Log.	leer

Ohne beide Schlüssel bleibt der Schutz in diesem Verkaufskanal inaktiv; das Log meldet das als Fehler.

Karte „Darstellung“

Feld	Optionen	Standard
Widget anzeigen	„Nur wenn ein Klick nötig ist“: für die meisten Besucher unsichtbar. „Immer“: kleines Feld mit Häkchen.	Nur wenn ein Klick nötig ist
Farbschema	Automatisch (folgt hellem oder dunklem Modus des Besuchers), Hell, Dunkel	Automatisch
Größe	Flexibel (volle Formularbreite), Normal (300 px), Kompakt (150 px)	Flexibel

- **Schmale Spalten.** Ist der Platz kleiner als 300 px, wechselt das Widget von selbst auf kompakt – etwa im Footer.
- **Sprache.** Das Widget spricht die Sprache des Verkaufskanals, nicht die des Browsers.
- **Hinweistexte.** Meldungen wie „Die Sicherheitsprüfung ist fehlgeschlagen“ kommen aus Textbausteinen (Deutsch, Englisch) und lassen sich unter **Einstellungen › Textbausteine** anpassen.

7 Prüfung auf dem Server

Was passiert, wenn das Token fehlt – und was, wenn Cloudflare schweigt.

Karte „Prüfung auf dem Server“

Feld	Bedeutung	Standard
Wenn Cloudflare nicht erreichbar ist	„Durchlassen und Warnung ins Log schreiben“ oder „Formular ablehnen“. Gilt bei Zeitüberschreitung (4 Sekunden), kaputter Antwort, internem Cloudflare-Fehler und bei fehlenden oder falschen Schlüsseln.	durchlassen
Domain des Tokens prüfen	Lehnt Tokens ab, die Cloudflare für eine andere Domain ausgestellt hat. Mit Testschlüsseln aus lassen.	aus

Die möglichen Ergebnisse

- **Bestanden** – Cloudflare bestätigt das Token; das Formular wird normal verarbeitet.
- **Abgewiesen** – kein, ungültiges, abgelaufenes oder bereits verbrauchtes Token. Gilt immer, unabhängig von der Einstellung oben.
- **Nicht prüfbar** – Cloudflare antwortet nicht oder die Schlüssel stimmen nicht. Je nach Einstellung durchgelassen oder abgelehnt.

> **DURCHLASSEN IST KEIN SCHLUPFLOCH**
>
> Ein Bot kann den Fall „nicht prüfbar“ nicht herbeiführen – ein gefälschtes Token beantwortet Cloudflare als ungültig. Durchgelassen wird nur, wenn Ihr Server Cloudflare wirklich nicht erreicht. So gehen bei einer Störung **keine Bestellungen und Registrierungen verloren**.

8 Store-API und Headless

Warum die Hintertür über die API zubleibt – und wie eigene Frontends das Token mitschicken.

Shopware prüft Captchas nur in der Storefront. Die Store-API braucht lediglich den Zugangsschlüssel des Verkaufskanals, und der steht in jedem Seitenquelltext. Ohne zusätzlichen Schutz könnten Bots den Newsletter oder die Registrierung direkt über die API aufrufen. Mit „Auch die Store-API schützen" verlangen diese Aufrufe ebenfalls ein Token:

Store-API-Route	Schalter
POST /store-api/newsletter/subscribe	Newsletter-Anmeldung
POST /store-api/account/register	Registrierung und Gastkauf
POST /store-api/contact-form	Kontaktformular
POST /store-api/revocation-request-form	Widerrufsformular
POST /store-api/account/login	Anmeldung (Login)

Token mitschicken

```
POST /store-api/newsletter/subscribe
sw-access-key: <Zugangsschlüssel>
sw-turnstile-token: <Token aus dem Turnstile-Widget>
```

Alternativ als Feld **cf-turnstile-response** im Body. Ohne gültiges Token antwortet die API mit **403** und dem Fehlercode **BMANIA_TURNSTILE__MISSING** bzw. **BMANIA_TURNSTILE__INVALID**; ist Cloudflare nicht erreichbar und „ablehnen" eingestellt, mit **503**.

> **EIGENES FRONTEND OHNE TURNSTILE?**
>
> Nutzt eine App oder ein Headless-Frontend diese Routen ohne Turnstile, schalten Sie „Auch die Store-API schützen" in diesem Verkaufskanal aus. Formulare der Storefront werden dabei **nicht doppelt** geprüft.

9 Betrieb: Cache, Log, Updates

Was im laufenden Betrieb zu beachten ist – vom Theme-Build bis zur Deinstallation.

Theme und Cache

- **Theme neu kompilieren** nach Installation und Updates, weil das Plugin Storefront-JavaScript mitbringt.
- **Einstellungen wirken ohne Theme-Build.** Shopware leert die betroffenen Seiten-Caches nach dem Speichern selbst; das kann einige Minuten dauern. Prüfen Sie kurz danach besonders den Footer.

Log

Das Plugin schreibt in eine eigene Datei **var/log/bmania_turnstile_<Umgebung>.log** (14 Tage). Darin stehen Route, Verkaufskanal und die Fehlercodes von Cloudflare – **nie Tokens oder Schlüssel**. Fehlende oder falsche Schlüssel erscheinen als ERROR, Ausfälle bei Cloudflare als WARNING.

Cookie-Manager und Content-Security-Policy

- **Cookie-Manager.** In aktiven Kanälen erscheint „Spam-Schutz (Cloudflare Turnstile)“ unter „Technisch erforderlich“ (ab Shopware 6.7.3).
- **CSP.** Setzt Ihr Server eine Content-Security-Policy, muss sie **challenges.cloudflare.com** für Skripte und Frames erlauben.

Updates und Deinstallation

- **Updates** behalten alle Einstellungen; danach das Theme neu kompilieren.
- **Deinstallation** entfernt Widget und Prüfung sofort. Ohne „Daten behalten“ löscht Shopware auch die Plugin-Einstellungen. Der Shopware-Honeypot bleibt unberührt.

10 Ihre Prüfpflicht: das Ergebnis kontrollieren

Was das Plugin nicht für Sie beurteilen kann.

DAS PLUGIN SCHÜTZT – SIE VERANTWORTEN

Ob jedes Formular Ihres Themes das Widget anzeigt, ob alle Domains im Cloudflare-Widget stehen und wie Sie die Datenübertragung an Cloudflare in Ihrer Datenschutzerklärung beschreiben, kann das Plugin nicht prüfen. **Das bleibt Ihre Aufgabe.**

Die Runde nach der Einrichtung

1. **Jedes geschützte Formular absenden** – Newsletter (auch im Footer), Registrierung, Gastkauf, Kontakt, Widerruf. Kommt die gewohnte Bestätigung?
2. **Fehlendes Widget ernst nehmen.** Bindet ein Theme-Formular das Captcha-Template nicht ein, wird dort **jede Absendung abgewiesen**. Template einbinden oder das Formular abschalten.
3. **Jeden Verkaufskanal einzeln prüfen** – mit seiner Domain, auch mit und ohne www.
4. **Mobil testen** – auf einem echten Gerät, das Widget darf das Layout nicht sprengen.
5. **Datenschutzerklärung ergänzen.** Turnstile überträgt u. a. die IP-Adresse an Cloudflare; beim Absenden prüft Ihr Server das Token mit IP-Adresse bei Cloudflare.
6. **Log nach einem Tag ansehen.** Viele abgewiesene Tokens sind normal (Bots); ERROR-Einträge deuten auf falsche Schlüssel.

11 Häufige Fragen

Was Shopbetreiber am häufigsten wissen wollen.

- **Muss meine Domain über Cloudflare laufen?**

  Nein. Sie brauchen nur ein kostenloses Cloudflare-Konto und ein Turnstile-Widget mit Ihren Shop-Domains. DNS und Hosting bleiben, wo sie sind.

- **Sehen meine Kunden ein Captcha?**

  Meist nicht. Im Standardmodus erscheint das Widget nur, wenn Cloudflare unsicher ist – dann genügt ein Klick. Bilderrätsel oder Abtippen gibt es nicht.

- **Ein Kunde meldet „Die Sicherheitsprüfung war noch nicht abgeschlossen". Was tun?**

  Meist blockiert ein Werbeblocker challenges.cloudflare.com oder JavaScript ist aus. Ohne Turnstile lassen sich geschützte Formulare nicht absenden. Fehlt das Widget bei allen Besuchern, prüfen Sie Domain und Theme (Kapitel 3 und 10).

- **Was passiert, wenn Cloudflare ausfällt?**

  Standardmäßig werden Formulare nach 4 Sekunden angenommen und protokolliert, damit keine Bestellung verloren geht. Sie können stattdessen „ablehnen" wählen (Kapitel 7).

- **Kann ich Turnstile nur für den Newsletter nutzen?**

  Ja. Schalten Sie unter „Geschützte Formulare" alle anderen Formulare aus (Kapitel 5).

- **Wo bekomme ich Hilfe?**

  Über den Support im Shopware-Account oder direkt bei der Gründerkind GmbH unter dev@gruenderkind.com. Halten Sie Shopware-Version, Plugin-Version, betroffenes Formular und die passenden Zeilen aus dem Plugin-Log bereit.