User Guide

Compatibility: Prestashop v1.7.x – v9.x.x

For Module Version: 1.0.0

Intended Audience

The content of this document is designed to facilitate the users -managers, supervisors and others of **AI Fraud Detection Module.** A step-by-step instruction has been added to this document to help users to install the module on PrestaShop.

As a safe practice always, backup your files and database before installing any module on PrestaShop. If you are looking for someone to install the module, we can do it for you as well. Just go to the support section share the order id to expedite the installation process.

Once you have installed, please see the User Guide to help you understand on how to use the module to its full capacity. If you still have questions feel free to contact us on the support platform where you bought this module.

If you have any custom requirements feel free to touch base with us.

Contents

Getting Started!

Overview

FMM Fraud Protector is an advanced security engine that automatically scores every login, registration, and order to shield e-commerce stores from fraudulent activity. It intelligently routes traffic into three lanes, approve, review, or block—based on custom 0-100 risk thresholds. The module supercharges defense by integrating Google Gemini and OpenAI for AI-driven analysis alongside enterprise tools like reCAPTCHA Enterprise and device fingerprinting. Administrators can manage investigations through a centralized case management dashboard that provides a complete forensic timeline of every shopper session.

Compatible with: PrestaShop 1.7 to 9.x

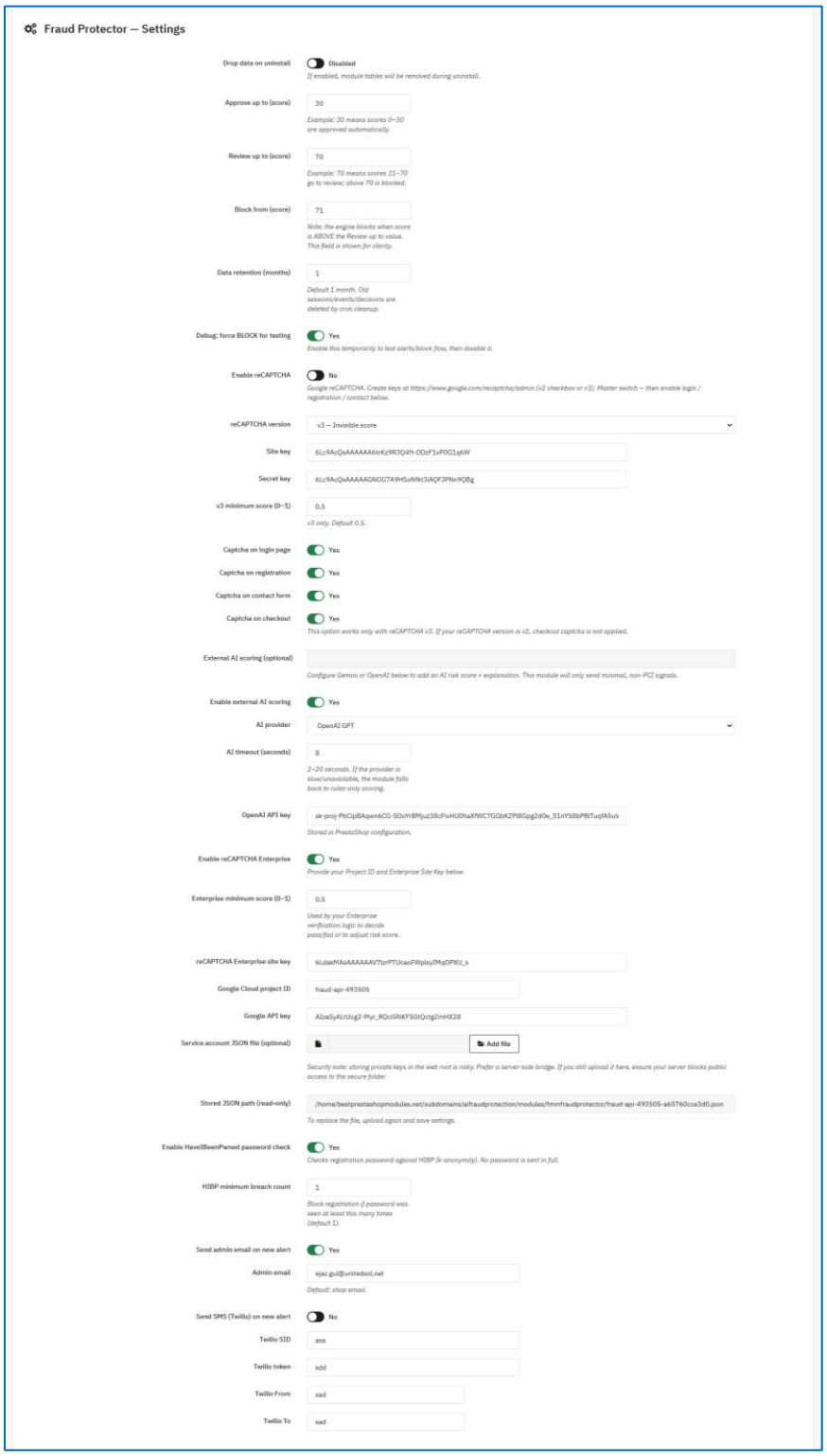
Installation Instructions

1. Go to Modules → Modules Manager → Click Upload a Module → Browse for Downloaded Module ZIP file and click Upload this module.
2. Click Proceed with Installation.
3. Make sure Cache is disabled in Advance Parameters → Performance.
4. Go to Modules → Modules Manager → AI Fraud Detection module

User Guide

Module Configuration:

After installing the module go to Module > Module Manager > AI Fraud Detection. Here you will see all the configuration for your module.



- **Drop data on uninstall**: When enabled, all module tables will be completely removed if you uninstall the module.
- **Approve up to (score)**: Sets the threshold for automatic approval; sessions with scores in this range (e.g., 0–30) are cleared immediately.
- **Review up to (score)**: Sets the threshold for manual intervention; scores in this range (e.g., 31–70) will generate an alert for your review.
- **Block from (score)**: Sets the threshold for automatic blocking; any session with a score at or above this value will be prevented from proceeding.
- **Data retention (months)**: Defines how long session logs are kept; data older than this limit (default is 1 month) is automatically deleted by the cron script.
- **Debug: force BLOCK for testing**: Temporarily force-blocks all sessions to verify your security block flows and layouts.

Google reCAPTCHA Settings

- **Enable reCAPTCHA**: Activates standard Google reCAPTCHA protection for your shop forms.
- **reCAPTCHA version**: Allows you to choose between **v2-Checkbox** (I'm not a robot) or **v3-Invisible score**.
- **Site Key**: The public key provided by Google for your reCAPTCHA configuration.
- **Secret Key**: The private key provided by Google for secure communication between your server and reCAPTCHA.
- **v3 Minimum Score (0-1)**: The minimum score required for a session to be considered valid when using reCAPTCHA v3.
- **Captcha on login page**: Enables CAPTCHA protection on the account login page.
- **Captcha on registration**: Enables CAPTCHA protection on the account registration page.
- **Captcha on contact form**: Enables CAPTCHA protection on the customer contact form.
- **Captcha on checkout**: Enables CAPTCHA protection during the checkout process (requires reCAPTCHA v3).

Note: Please check below on how to configure Google Capctha

External AI Scoring (Optional)

- **Enable external AI scoring**: Configures the module to use **Google Gemini** or **OpenAI** to analyze and score sessions during registration or alerts.
- **AI provider**: Selects which service (Gemini or OpenAI) will perform the external risk analysis.
- **AI timeout (seconds)**: The maximum time the module will wait for an AI response before falling back to local scoring rules.
- **Gemini/OpenAI API key**: Your unique API key for the selected AI service.

reCAPTCHA Enterprise

- **Enable reCAPTCHA Enterprise**: Activates advanced, enterprise-grade bot protection.
- **Enterprise minimum score (0-1)**: The required score threshold defined in your Google Enterprise configuration.
- **reCAPTCHA Enterprise site key**: Your unique Enterprise site key from the Google Cloud Console.
- **Google Cloud project ID**: Your specific Google Cloud project identifier.
- **Google API Key**: The API key used for Google Cloud service authentication.

- **Service account JSON file (optional)**: Allows you to upload a credentials file for more secure backend access to Google services.

Note: Please check below on how to configure Google Capctha Enterprise

Security & Alerts

- **Visitor data push (CRON URL)**: The endpoint URL used to trigger automated data cleanup and background tasks via a cron job.
- **Enable HaveIBeenPwned password check**: Instantly checks if a user's password has appeared in known data breaches during registration.
- **HIBP minimum breach count**: Prevents registration if a password has appeared in at least this many data breaches (default is 1).
- **Send admin email on new alert**: Automatically notifies the administrator via email whenever a new fraud alert is generated.
- **Admin email**: The specific email address where alert notifications will be sent.
- **Send SMS (Twilio) on new alert**: Automatically sends an SMS notification when a new alert is created.
- **Twilio SID / Token / From / To**: The necessary credentials and phone numbers to facilitate automated SMS alerts via Twilio.

1. Google Simple reCAPTCHA (v2 & v3)

This version uses the classic **reCAPTCHA Admin Console** to protect your forms with either a checkbox or an invisible score.

- **Step 1: Access the Console**: Visit the Google reCAPTCHA Admin Console and sign in with your Google account.
- **Step 2: Register Site**: Click the **"+" (Create)** icon. Enter a **Label** (e.g., "My Store") to identify your keys.
- **Step 3: Select Type**: Choose **reCAPTCHA v3** (Score-based) or **reCAPTCHA v2** ("I'm not a robot" Checkbox or Invisible).
    - *Note: Ensure the type you select matches the "reCAPTCHA version" dropdown in the module settings.*
- **Step 4: Add Domains**: Enter your store's domain (e.g., `mystore.com`) without the `https://` prefix.
- **Step 5: Get Keys**: Accept the Terms of Service and click **Submit**. Copy the **Site Key** and **Secret Key** into the module's corresponding fields.

2. Google reCAPTCHA Enterprise

Enterprise version is managed through the **Google Cloud Console** and offers more advanced bot detection features.

- **Step 1: Create a Project**: Go to the Google Cloud Console, click the project dropdown at the top, and select **New Project**.
- **Step 2: Enable API**: In the sidebar, go to **APIs & Services > Library**. Search for **"reCAPTCHA Enterprise API"** and click **Enable**.

- **Step 3: Create Enterprise Key**: Navigate to **Security > reCAPTCHA Enterprise** in the sidebar. Click **Create Key**.
    - Set **Platform Type** to "Website" and add your domain.
    - Copy the generated **Enterprise Site Key**.
- **Step 4: Obtain Project ID**: You can find your **Project ID** on the Cloud Console dashboard or at the top of the project selector.
- **Step 5: Create API Key**: Go to **APIs & Services > Credentials**. Click **Create Credentials > API Key**. Copy this into the **Google API Key** field in the module.
- **Step 6: Service Account (Optional)**: For high-security environments, go to **IAM & Admin > Service Accounts**. Create a new account with the **"reCAPTCHA Enterprise Agent"** role, create a **JSON Key**, and upload it to the module.

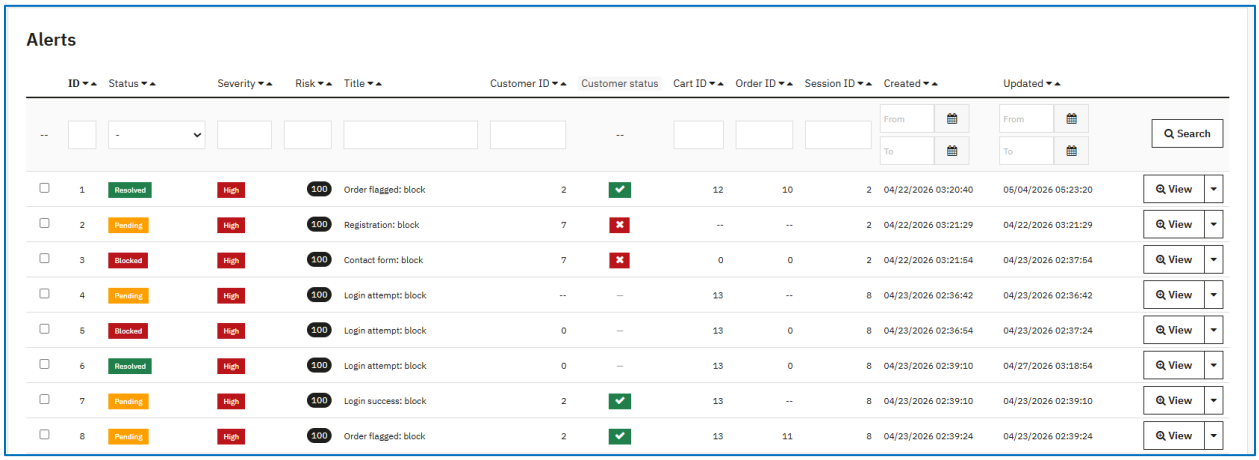
Quick Mapping for Module Settings:

Module Field	Source Location
Site Key / Secret Key	reCAPTCHA Admin Console (Simple v2/v3)
Google Cloud Project ID	Google Cloud Console Dashboard (Enterprise)
Enterprise Site Key	Security > reCAPTCHA Enterprise (Enterprise)
Google API Key	APIs & Services > Credentials (Enterprise)

How to view alerts and block users:

The Alerts section is your frontline defense, providing a real-time queue of all suspicious activities flagged by the system. Below is a breakdown of how to read the data and take action.

Note: we have not included auto blocked option as this can cause issues if we allow AI to make this decision, you need to manuly block users after assessing alerts.

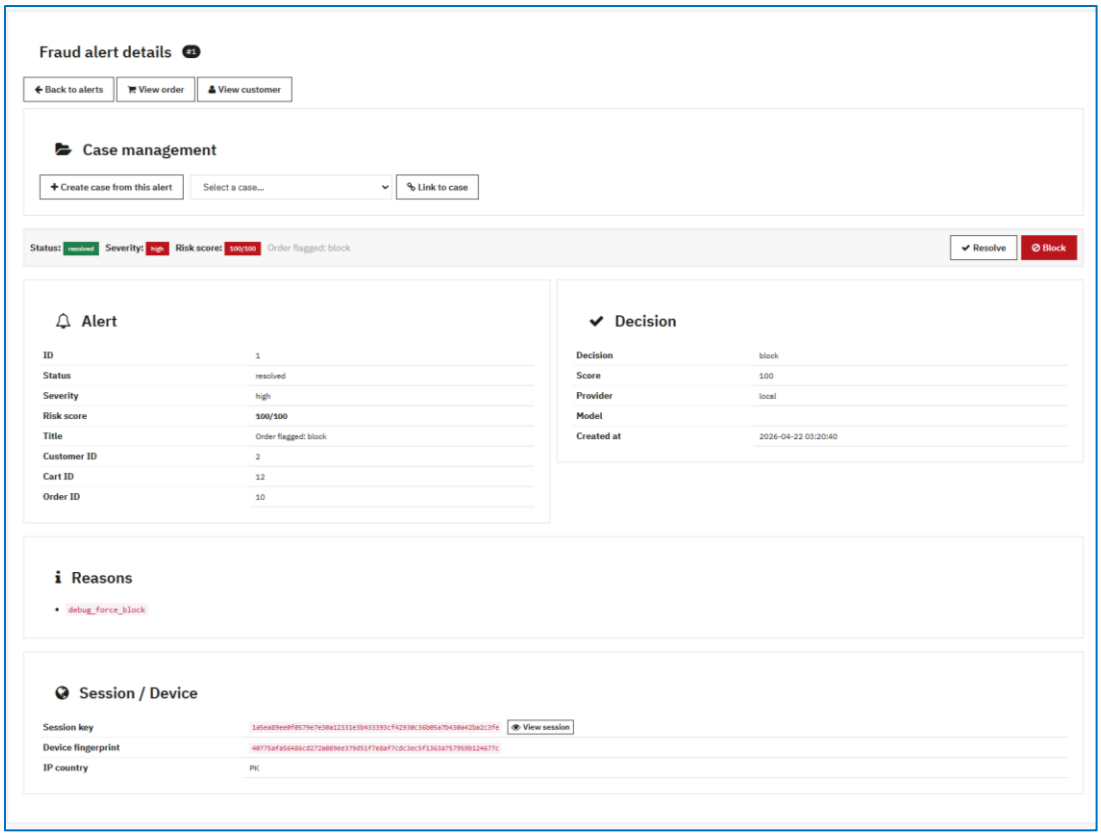


Alerts Listing (Queue View)

This view provides a high-level overview of recent activity based on your scoring thresholds.

- **ID**: The unique numerical identifier for each individual alert generated.
- **Status**: Indicates the current state of the alert, categorized as **Pending** (needs review), **Resolved** (cleared by admin), or **Blocked** (automatically or manually stopped).
- **Severity**: A color-coded priority level (e.g., **High**) based on the calculated risk.
- **Risk**: The 0–100 score assigned to the session; higher numbers indicate a higher probability of fraud.
- **Title**: Describes the specific action that triggered the alert, such as an **Order flagged**, **Registration**, or **Login attempt**.
- **Customer / Cart / Order ID**: Direct links to the associated shop data, allowing you to see exactly which account or purchase is under investigation.
- **Customer Status**: A visual indicator (Check/X) showing if the customer account is currently active or disabled.
- **Search / Filter**: Tools to quickly narrow down alerts by date range, specific IDs, or event titles.
- **View**: Opens the **Fraud Alert Details** page for a deep-dive investigation.

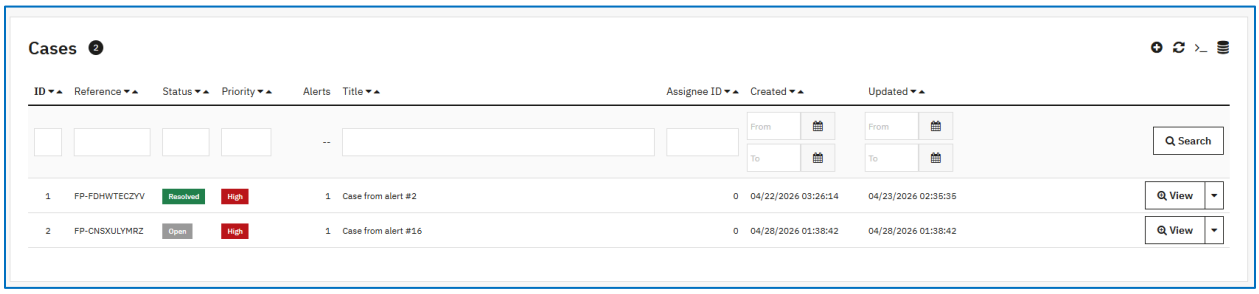
Fraud Alert Details (Investigation View)



Once you click **View**, you can access granular data to make an informed decision.

- **View Order / View Customer**: Quick-action buttons to jump directly to the native PrestaShop pages for the related order or user profile.
- **Case Management**: Allows you to **Create a case from this alert** to start a formal investigation or **Link to case** to group it with other related suspicious activities.
- **Resolve**: A manual action button to clear the alert and mark the activity as legitimate.
- **Block**: A manual action button to immediately stop the user and prevent further transactions or logins.
- **Alert & Decision Tables**: Technical summaries showing who made the decision (e.g., **Local** rules or **AI** provider) and the exact timestamp of the event.
- **Reasons**: A dedicated section listing the specific rules or triggers (e.g., `debug_force_block`) that caused the risk score to spike.
- **Session / Device**: Forensic evidence including the **Device Fingerprint**, **Session Key**, and **IP Country**.
- **View Session**: A one-click link to the full **Sessions** log to see the user's complete chronological journey on your site.

Cases Section:

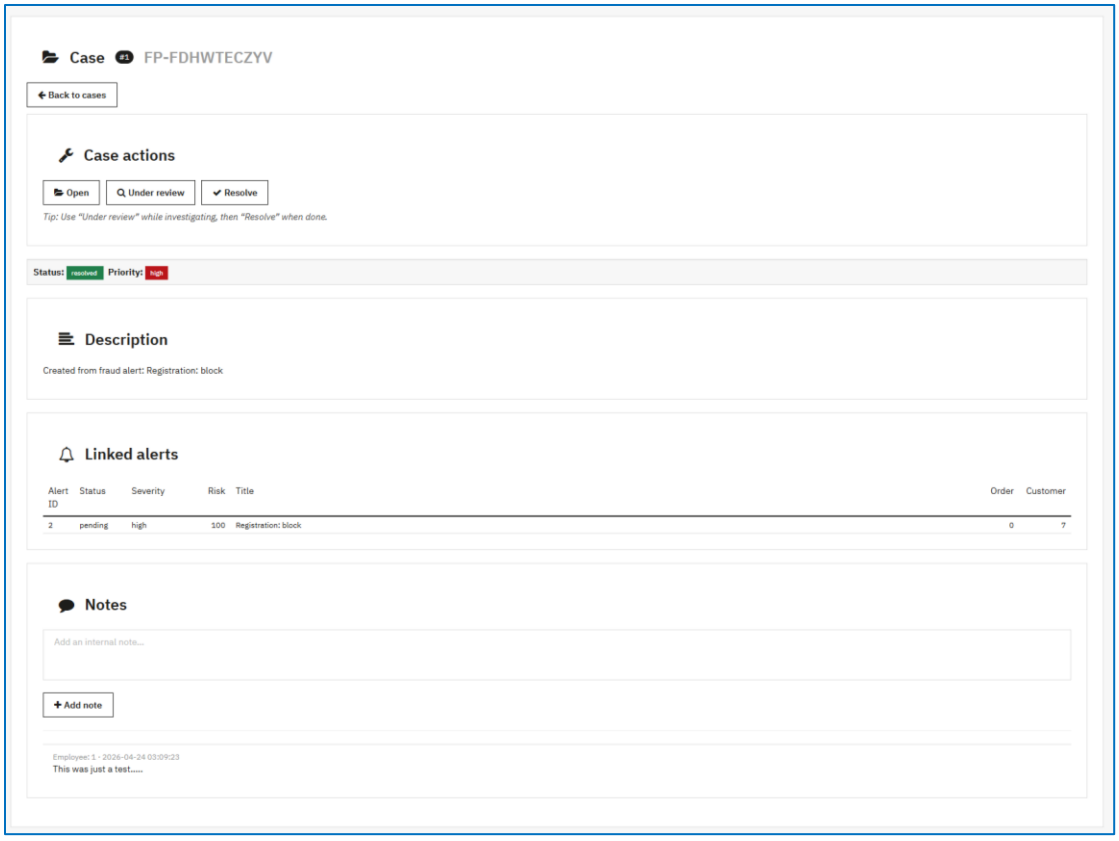


The **Cases** section acts as your investigative headquarters, allowing you to group related suspicious activities into a single file for organized tracking and team collaboration.

Cases Listing (Headquarters View)

This list provides an overview of all active and historical investigations.

- **ID**: The unique numerical identifier for the case.
- **Reference**: A unique alpha-numeric string used for easy search and cross-referencing (e.g., FP-FDHWTECZYV).
- **Status**: The current stage of the investigation, such as **Open**, **Under review**, or **Resolved**.
- **Priority**: Indicates the urgency of the case, typically categorized as **High**, Medium, or Low.
- **Alerts**: Shows the total number of individual fraud alerts currently linked to this case.
- **Title**: A brief description, often identifying which specific alert triggered the creation of the case.
- **Assignee ID**: Identifies the specific team member currently responsible for the investigation.
- **Created / Updated**: Precise timestamps showing when the investigation began and when it was last modified.
- **View**: Opens the **Case Detail** page to manage the investigation.



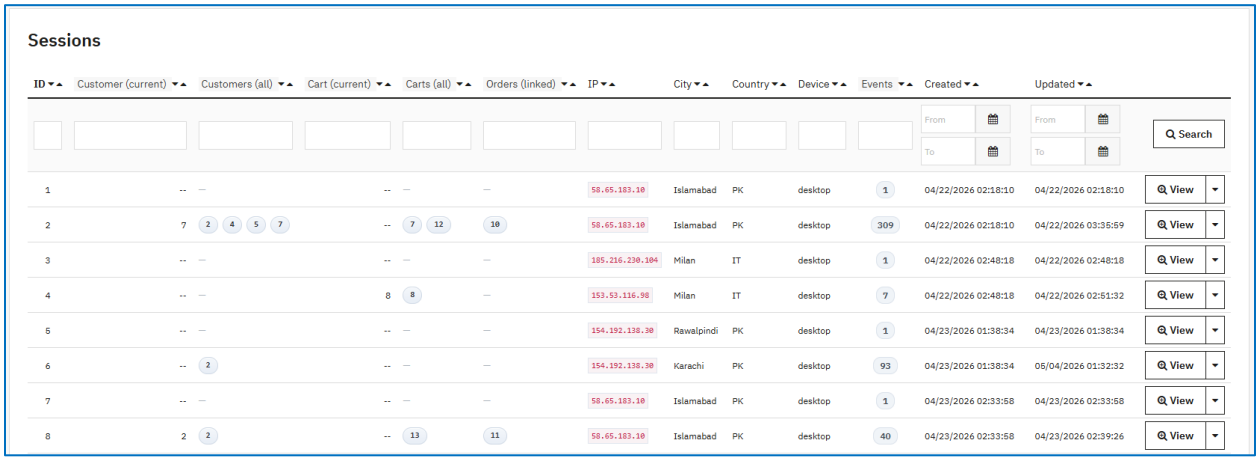
Case Detail View (Investigation Workspace)

The detail page provides the tools necessary to manage the lifecycle of a fraud investigation.

- **Case Actions**: Use these buttons to manage the investigation workflow:
  - **Open**: Mark a new or dormant case as active.
  - **Under review**: Indicate that the case is currently being investigated.
  - **Resolve**: Close the case once a final decision has been made.
- **Description**: Displays the origin of the case, such as the specific fraud alert that initially triggered the investigation.
- **Linked alerts**: A detailed table listing every individual alert associated with this case. This includes the **Alert ID**, **Severity**, **Risk Score**, and links to the specific **Order** or **Customer** involved.
- **Notes**: A collaborative area for internal team communication.
  - **Add note**: Allows you to record findings, evidence, or internal decisions.
  - **History Log**: Maintains a chronological record of all notes, including the employee's name and the exact time the comment was added.

Sessions Section:

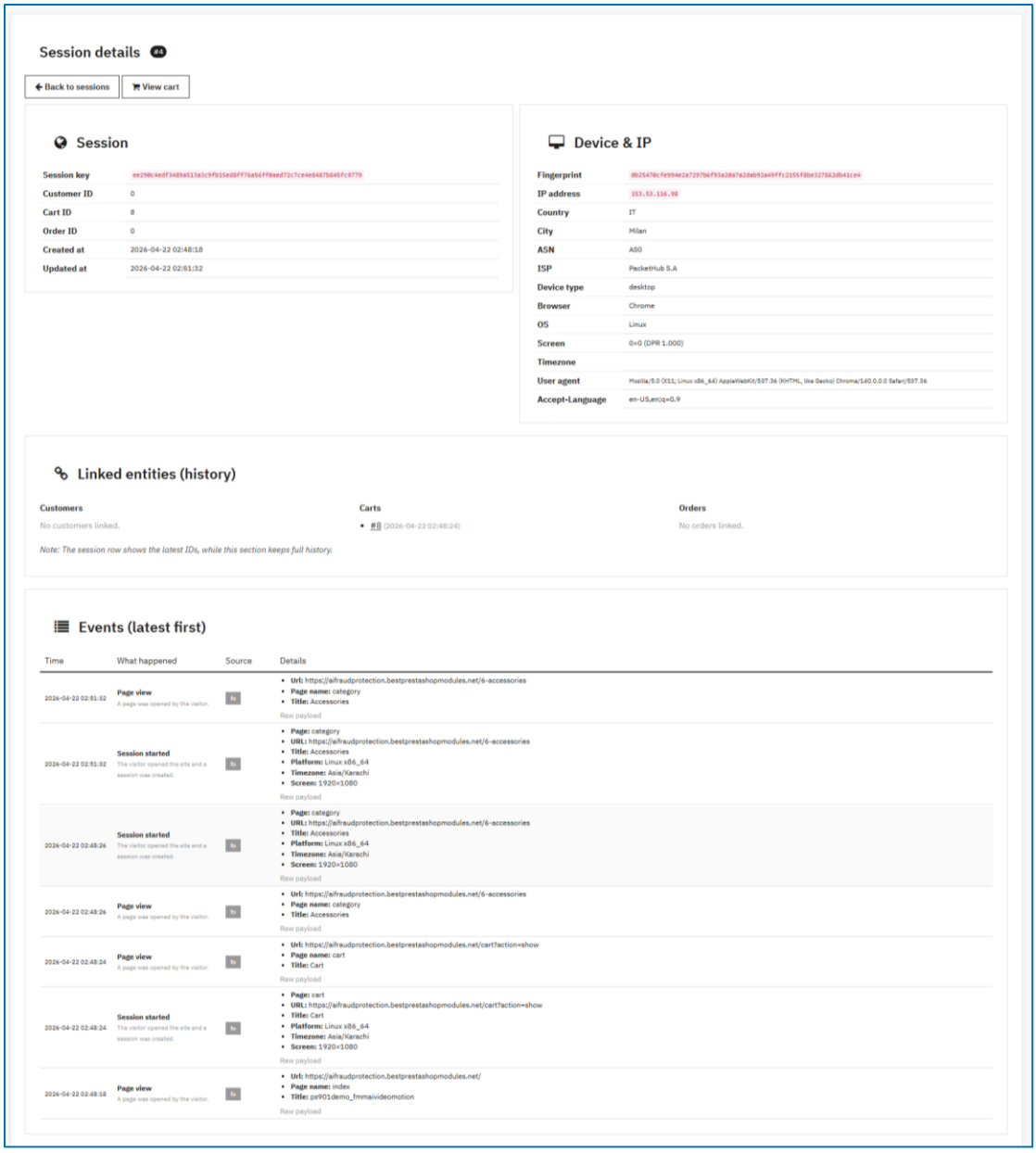
The **Sessions** section acts as a master activity log, recording every interaction a visitor has with your store. It provides the deep forensic data needed to identify bot patterns and suspicious shopper behavior.



Sessions Listing (Log View)

This view provides a high-level summary of all active and past visitor sessions.

- **ID**: The unique numerical identifier for the visitor's session.
- **Customer / Customers (all)**: Shows the current logged-in user and any other customer accounts that have been accessed during this specific session. IDs are displayed as clean chips for easy readability.
- **Cart / Carts (all)**: Displays all shopping carts associated with the session, allowing you to see if a single visitor is cycling through multiple carts.
- **Orders (linked)**: Lists any completed orders tied to this session.
- **IP**: The visitor's IP address; highlighted in red for quick identification.
- **City / Country**: The geolocation data derived from the IP address.
- **Device**: Identifies the hardware used (e.g., **desktop** or mobile).
- **Events**: The total number of individual actions (page views, clicks, etc.) performed during the session. High event counts can often indicate bot activity.
- **Created / Updated**: Precise timestamps for when the session started and the last recorded activity.
- **View**: Opens the **Session Details** page for a full forensic breakdown.



Session Details (Forensic View)

The detail page allows you to inspect the "DNA" of a specific session to verify if the visitor is human or a bot.

- **View Cart**: A quick-action button to jump directly to the active shopping cart in the PrestaShop back office.
- **Session Table**: Provides the unique **Session Key** and the primary IDs for the customer, cart, and order currently linked to the session.
- **Device & IP (Forensics)**: An exhaustive technical breakdown used for identification:
    - **Fingerprint**: The unique hardware/browser signature assigned to the user.
    - **ASN / ISP**: The network provider information, helpful for spotting data center or proxy traffic.

    - **Screen / Timezone**: Technical browser details that help identify automated scraping tools.
    - **User Agent**: The full string identifying the browser version and operating system.
- **Linked entities (history)**: A historical log of every customer account, cart ID, and order ever touched by this session, providing a clear map of the visitor's impact on your store.
- **Events (latest first)**: A chronological timeline of the user's journey.
    - **Time**: The exact moment the action occurred.
    - **What happened**: The type of event (e.g., **Page view**, **Session started**, **Order placement**).
    - **Details**: Granular data for each event, including the specific **URL** visited and the **Page name**. Use this to trace the exact path a suspicious user took through your shop.

Disclaimer

It is highly recommended to backup your server files and database before installing this module.

No responsibility will be taken for any adverse effects occurring during installation.

It is recommended you install on a test server initially to carry out your own testing.

Support

If you need more information or have any questions or problems, please refer to our support helpdesk:

You can log a ticket and a support technician can assist you further.

Customization

If you have requirements that are not covered by our module and you need to have our module customized, feel free to contact us through support helpdesk.