

# Brand safety

- [Brand safety solutions on Eskimi](#)
- [Brand safety update](#)
- [Eskimi DSP Anti-fraud Settings](#)
- [How to enable Brand Safety on a campaign level](#)

# Brand safety solutions on Eskimi

Brand safety refers to the measures taken to ensure that a brand's advertising will not appear alongside content that could harm the brand's reputation or be offensive to its target audience. This can include content that is violent, hateful, sexually explicit, or promotes illegal activities.

Brand safety is an important consideration when placing advertising, as it helps to protect the brand image and reputation. It can also help to prevent legal issues from arising from advertising being placed next to inappropriate content. This can be achieved through various ways such as using brand safety tools, monitoring the placements of ad, using keywords filtering, context analysis and more.

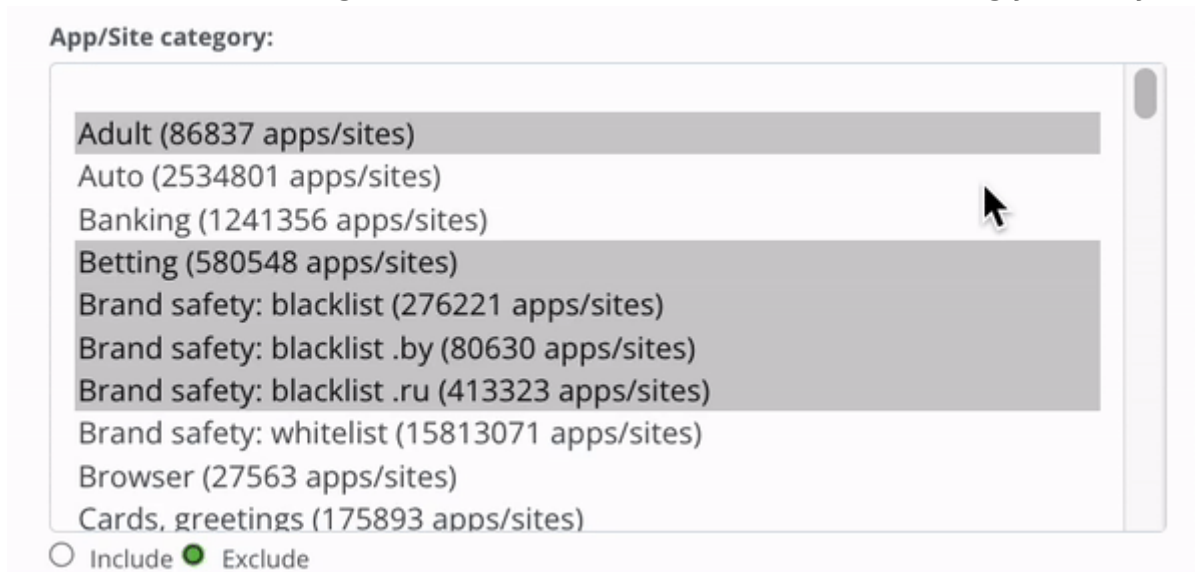
Eskimi DSP supports 5 different layers of brand safety tools which ensures relevant and brand-safe environment.



## Traffic source content information

### Category exclusion

The first layer consists of checking the general website content from the information provided by the exchanges and/or publishers. All placements are categorized, and sensitive categories - such as adult content, betting, arms, violence, etc. - are excluded accordingly in every campaign:



Picture 1 - Categories that excluded in Eskimi DSP as default

## Pre-optimization based on historical data

Besides the category exclusion, campaigns are pre-optimized by using historical placement stats to exclude sites or/and apps that showed poor performance in the past. Also, this tool works both ways - it is possible to run on sites/apps that showed good performance. In other words, general brand safety solutions are done for each brand and its advertising.

**Limitations:** Information that comes from an exchange/publisher is not always accurate.

**Addressing limitations:** Employing additional internal tools to ensure brand safety.

---

## URL Keyword checking

Unfortunately, traffic source content information isn't enough when facing placement content. A lot of news sites are categorized as not sensitive, although they are full of sensitive and disturbing information that may harm the brand. To move forward with an in-depth solution, Eskimi DSP launched a URL keyword checking tool. If an URL contains keywords from a negative keywords list, an impression will not be purchased and the ad won't be showed near such an article.

**Limitations:** 1) URL doesn't include any negative keywords. 2) Apps traffic cannot be checked.

**Addressing limitations:** 1) Reviewing website content. 2) Whitelist/Blacklist for apps.

---

## Site content reviewing for keywords

The keyword checking an URL helps to analyse the content. However, it doesn't safeguard from lists that don't have a negatively listed keyword in the URL but have a lot of unwanted material in the content itself. To bring brands to an even higher brand safety solution, ESKIMI DSP is working on an on-site content analysis that will analyse the content of an article on the homepage.

**Limitations:** 1) Content doesn't include any negative keywords. 2) Apps traffic cannot be checked.

**Addressing limitations:** Whitelists/Blacklists

---

## Human curated whitelist/blacklist

By excluding sensitive topics, we limit ads to certain categories. However, some brands are solely focused on exact categories. On Eskimi DSP it is possible to whitelist and blacklist sites/apps based on brand preference. This means that ads will appear or won't appear on (un)wanted placements.

**Limitations:** 1) Different definitions when understanding avoidable content. 2) Whitelist limits traffic. 3) Human mistakes.

**Addressing limitations:** Align and approve whitelist with the client.

---

## External tools & services

In addition to our in-house brand safety solutions, we are working with 3<sup>rd</sup> party brand safety platforms such as DoubleVerify, Integral ad Science, The Media Trust, and many other tools if a client requests.

To sum it up, brand safety should be one of the highest priorities for the brand and for the platforms that they are partnering with. With an always growing demand, Eskimi DSP is working on in-dept solutions to fill the client's needs. As the market is getting more aggressive and competitive these deeper solutions are key when delivering good services.

**Limitations:** 1) Extra costs when using selected tools. 2) Potential increase in CPM price. 3) Limited abilities to verify app traffic.

# Brand safety update

## Brand safety update:

Exclude 'Strict' and 'suspicious' was merged into 'Exclude'. You only have 'exclude' or 'include' in Brand safety now. Here's how include/exclude works now. Will add to manual a bit later - please ask questions if any and will adjust accordingly. **Step 1.** You create a brand safety set of some words you want to target or want to avoid

- If you choose 'find in URL', system will check if the keyword is in full URL and exclude/include the URL

For example, if you exclude a set that contains murder, and bid request comes from [randomsite.com/murder](https://randomsite.com/murder), Eskimi will not bid

- If you choose 'Find in content', system will crawl relevant campaign sites and only show ads if domain was crawled and no 'murder' was in that domain

E.g. if [randomsite.com/randomsite](https://randomsite.com/randomsite) comes in a bid, Eskimi will we will not bid till our crawler checks what's in that site. Once we do the check, we will see if 'murder' is part of the content or not, and include/exclude site accordingly. **Match types:**

- Contains type match: looks for similar looking words. if you have 'murder' in the set, all similar words will be added: '**murderers, murderous, randomsomethingmurder**, etc.'
- Exact word type match: looks for exact words. If you have 'murder' in the set, it will only look for 'murder', not 'murderers' or 'murderous'.

## Step 2. Choose on campaign approval

- If package is 'find in URL', campaign starts using the URL for validation
- if package is 'find in content', crawler kicks in and starts checking relevant sites, and bidding only once relevant sites are checked. So there might be a delay in checking what content is hidden behind the site URL.

### Tip #1:

Check if your keyword set doesn't have single letters, words of a few letters or similar. Having such would cause 'type match' to exclude lots and lots of traffic.

E.g. if you added letter 'a' to the set and choose 'contains type match', all sites containing letter 'a' would be excluded. That's a lot of sites, as you can imagine **Tip #2:**

brand safety keywords only work on full URL. E.g. [randomsite.com/randomsite](https://randomsite.com/randomsite), [randomsite.com/notsorandom](https://randomsite.com/notsorandom), [randomsite.com](https://randomsite.com) are treated as 3 different sites

# Eskimi DSP Anti-fraud Settings

In today's digital advertising landscape, combating fraud is a critical priority for maintaining the integrity and effectiveness of campaigns. Major industry players often rely on custom solutions for fraud detection, while others turn to trusted third-party services such as IAS, DoubleVerify, Picalate, and HUMAN. At our company, we have developed an internal anti-fraud tool and collaborate with global exchanges that employ their own or third-party solutions to filter out fraudulent activities. This results in a robust, multilayered fraud detection system, combining our internal tools with the "filtered" traffic from exchanges and SSPs. As an Eskimi DSP user, leveraging the anti-fraud settings is essential to maximize the efficiency and credibility of your advertising efforts. Below, we provide a detailed overview of each option available on the approval page and their technical functionalities.

## 1. Exclude New (Non-DMP) Users

This setting is designed to filter out users who don't have a Data Management Platform (DMP) ID in the Eskimi system. By enabling this option, your campaign will prioritize users already present in our DMP, enhancing the targeting precision and reducing the risk of fraudulent activities.

## 2. Exclude Users with High Daily Apps/Sites Count

Eskimi DSP monitors bid requests for each user, and this setting kicks in when a user's daily Apps/Sites count surpasses a predefined threshold. By excluding users with unusually high activity, the system mitigates the risk of engaging with potentially fraudulent or non-genuine users.

## 3. Exclude Users with High Daily Page Views

Similar to the previous setting, Eskimi DSP evaluates the number of bid requests per user. If a user's daily page views exceed a specified limit, the system excludes them from winning bids. This helps maintain campaign quality and ensures engagement with authentic users.

## 4. Exclude Fake Clickers

To combat click fraud, Eskimi DSP employs a code implementation that distinguishes between genuine users and bots mimicking legitimate clicks. Users exhibiting suspicious clicking behavior are automatically disqualified from winning bids, safeguarding your campaign from fraudulent activities.

## **5. Exclude Domain Spoofers**

This setting targets domains attempting to mimic popular websites with slight variations in variables or letters. By excluding these spoofed domains, such as forb1s.com instead of forbes.com, Eskimi DSP fortifies your campaign against potential fraudulent traffic.

## **6. Exclude ads.txt Mismatching Apps/Sites**

This anti-fraud measure ensures that bid requests are accepted only from apps/sites where the Exchange or SSP sending the bids is present in the ads.txt list. For instance, if a popular website like foxnews.com lacks Eskimi in its ads.txt list, enabling this option will reject bids originating from Eskimi SSP via foxnews.com, preventing potential fraud.

By leveraging these anti-fraud settings, Eskimi DSP empowers users to maintain campaign integrity, enhance targeting accuracy, and safeguard against various fraudulent activities in the digital advertising landscape.

# How to enable Brand Safety on a campaign level

Brand safety refers to the measures taken to ensure that a brand's advertising will not appear alongside content that could harm its reputation or be offensive to its target audience. This can include content that is violent, hateful, sexually explicit, or promotes illegal activities.

---

## Brand Safety for your campaigns

You can ensure Brand Safety for your campaigns by using either keyword targeting or apps/sites categories, or both. These features work together to safeguard your brand's image and prevent your ads from appearing near undesirable content.

## How to exclude Keywords for your campaigns

To enable brand safety feature in your campaign, you need to:

1. Create a keyword list of certain words you want to exclude.
2. Enable Brand Safety on a campaign level.

## Keyword Lists

The keyword list can be created on the [Keywords page](#):

1. Visit the Keywords page under Tools.
2. Click Create at the top right.
3. Add "Title" to your Keyword list.
4. Select at least one "Context option".
  - If you choose "find in URL", the system will check if the keyword is in full URL and exclude the URL.  
E.g. if you exclude a set that contains murder, and a bid request comes from randomsite.com/murder, Eskimi will not bid on this request.
  - If you choose "Find in content", the system will crawl relevant campaign sites and only show ads if the domain was crawled and no 'murder' was in that domain. E.g. if randomsite.com comes in a bid, Eskimi will not bid till our crawler checks what's in that site. Once we do the check, we will see if 'murder' is part of the content or not, and include/exclude the site accordingly.

*Note: both of these options can be selected. When both options are selected, the URL and page content are checked for keywords.*

5. Select "Match option".
  - Contains type match: looks for similar looking words. if you have 'murder' in the set, all similar words will be added: '**murderers**, **murderous**, randomsomething**murder**, etc.'
  - Exact word type match: looks for exact words. If you have 'murder' in the set, it will only look for 'murder', not 'murderers' or 'murderous'.
6. Upload keywords.
7. Click Save.

Check if your keyword set doesn't have single letters, words of a few letters or similar. Such setup would cause "contains type match" to exclude lots and lots of traffic. E.g. if you added letter 'a' to the set and chose 'contains type match', all sites containing letter 'a' would be excluded. That can be a lot of sites.

Keywords only work on full URLs. e.g. randomsite.com/randomsite, randomsite.com/notsorandom, randomsite.com are treated as 3 different sites.

## Excluding keywords on a Campaign

Once you have created a set of keywords, you can enable brand safety for your campaign.

1. Open the selected campaign.
2. Scroll down to Brand safety.
3. Select one or more keyword sets under the Keywords targeting.
4. Click Save.

< BACK TO LIST

## Create Campaign group

Name & Type	<h3>Form navigation</h3> <ul style="list-style-type: none"><li>Name &amp; Type<ul style="list-style-type: none"><li>Campaign goal</li><li>Primary campaign objective</li><li>Secondary campaign objective</li></ul></li><li>Launch date &amp; Budget</li><li>Location &amp; Audiences</li><li>Brand safety<ul style="list-style-type: none"><li>Contextual targeting</li></ul></li><li>Campaign purpose</li><li>Platforms, Telco &amp; Devices</li><li>Deals &amp; packages</li><li>Landing &amp; Creatives</li><li>Buttons</li></ul> <p>Created by: Eskimi - Kamile Last updated by: N/A Created: 2024-01-19 09:35:06 (GMT+3) Last updated: N/A</p>
Campaign goal	
Primary campaign objective	
Secondary campaign objective	
Launch date & Budget	
Location & Audiences	
Brand safety	
Apps/Sites categories <input type="text"/>	
Keywords <input type="text"/>	
Select any <input type="text"/>	

Keep in mind that if [contextual targeting](#) is enabled on the same campaign, both settings will be taken into account. If both brand safety and contextual targeting keyword sets have the same words, the matching keywords will be excluded. Eskimi ensures that the Brand Safety setting is always prioritized.

Once the brand safety settings are set on a campaign:

- If the keyword set is 'find in URL', the campaign starts using the URL for validation.
- If the keyword set is 'find in content', the crawler kicks in and starts checking relevant sites, and bidding only once relevant sites are checked. So there might be a delay in checking what content is hidden behind the site URL.

***Please note that this feature is only available for site placements and not applicable for apps.***

## How to exclude apps/sites categories for your campaigns

The apps/sites category feature helps users target ads based on the market verticals of the page. Apps/sites categories contain already pre-created lists of domains and app bundles of related topics such as Finance, Sports or Games. These categories cover 98.6% of supply. Categories are

grouped into two bigger groups - General topics & Sensitive topics accordingly.

To setup category targeting, you need to:

1. Open the selected campaign.
2. Scroll down to Brand Safety.
3. Select categories under the Apps/Sites categories.
4. Click Save.

The screenshot shows the 'Create Campaign group' form in the Eskimi interface. The form is divided into several sections: 'Name & Type', 'Campaign goal', 'Primary campaign objective', 'Secondary campaign objective', 'Launch date & Budget', 'Location & Audiences', and 'Brand safety'. The 'Brand safety' section is expanded, showing 'Apps/Sites categories' with a search bar and two options: 'General topics' (unchecked) and 'Sensitive topics' (checked). Below this is a 'Keywords' section with a 'Select any' dropdown. On the right side, there is a 'Form navigation' panel with a list of sections: 'Name & Type', 'Campaign goal', 'Primary campaign objective', 'Secondary campaign objective', 'Launch date & Budget', 'Location & Audiences', 'Brand safety' (highlighted), 'Contextual targeting', 'Campaign purpose', 'Platforms, Telco & Devices', 'Deals & packages', 'Landing & Creatives', and 'Buttons'. At the bottom right, there is a metadata box showing 'Created by: Eskimi - Kamile', 'Last updated by: N/A', 'Created: 2024-01-19 09:35:06 (GMT+3)', and 'Last updated: N/A'.

Keep in mind that if apps/sites categories targeting is enabled under [contextual targeting](#) on the same campaign, both settings will be taken into account. If both brand safety and contextual targeting have the same categories selected, the matching domains or apps bundles will be excluded. Eskimi ensures that the Brand Safety setting is always prioritized.

Our categorization system now works on two levels:

- Page-level: Our AI engine analyzes individual page content to determine precise categories (e.g., a sports article on a news site will be categorized as "Sports")
- Domain/app bundle level: Used as a fallback when page-level analysis is not yet available

The system prioritizes page-level categorization for better targeting precision, while maintaining domain-level categorization for comprehensive coverage. Note that we continue to crawl page content for keyword targeting as well.