# Hashed Mobile Advertising ID Targeting

At Eskimi the key element is to provide clients privacy safe solutions. This is why Eskimi can provide clients to use their hashed first party data which provides privacy that clients are looking for.

---

## Hashed first-party data

Eskimi supports only **sha256** hashing. This is a well known cryptographic hash that turns a 36-character device ID into a 64-character hash.

**Example of unhashed device ID:**

00001928-4f63-4923-8ce0-a1e2c2517385

**Example of sha256 hashed device ID:**

335a0a471e13c7773712a038576f6186c7df6975ee3f91500c97112a44135e0f

---

## Why hashed first-party data is important?

**Privacy.** They key goal of hashed first-party is to ensure privacy for the data that clients share. By providing the opportunity to upload hashed device IDs Eskimi provides privacy first solution to the clients.

**Manual Appsflyer Audience.** Hashed first-party data upload enables advertisers to manually upload audience from Appsflyer. This wasn't possible before as Eskimi was able to only take up unhashed device IDs. While now clients can take their first-party data from Appsflyer and upload it on Eskimi dashboard and use the data during programmatic advertising.

**Easier first-party monetisation.** Clients won't need to unhashed their first party data if they have it hashed. This enables easier first party monetisation.

---

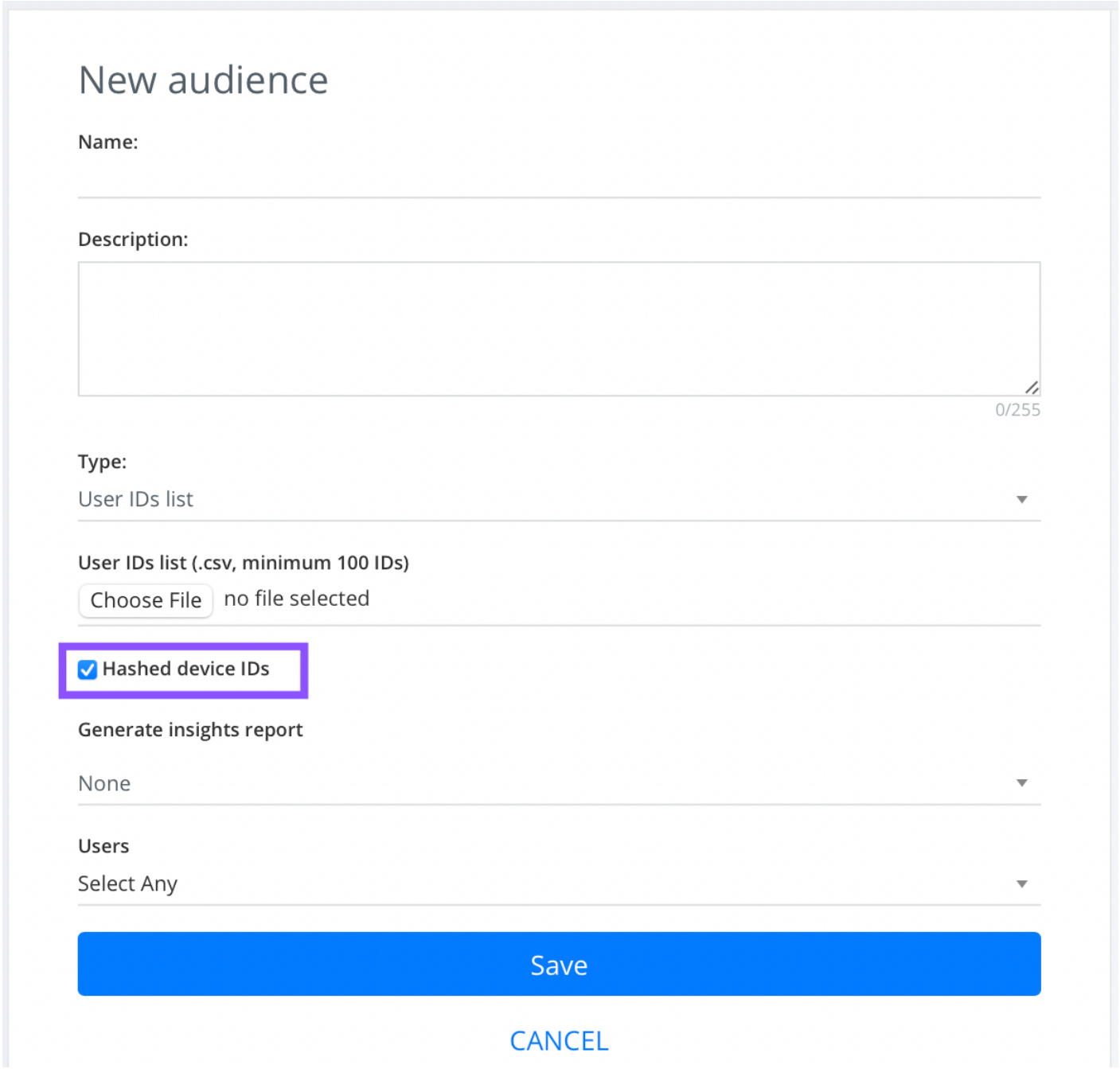
# How hashed first-party data is uploaded?

Hashed device IDs are uploaded the same way as unhashed ones. In Eskimi dashboard you have to go to:

*Tools -> Audiences -> Add Audience -> Under Audience Type select: Advertiser IDs list -> Upload a .csv file of hashed device IDs (minimum 100 IDs) -> check Hashed device IDs (as in the example).* By doing so you will inform the system that you uploaded hashed device IDs which will make the matching easier.

After the audience is created it will take around 15 minutes for the system to do the matching. After that audience can be added as targeting.

Keep in mind that clients still can only use hashed device IDs so the uploaded audience will be compatible with targeting that uses device IDs (app, operator, device and etc.)




# How to hash device IDs?

Device IDs can be hashed by using various online tools. For example: https://emn178.github.io/online-tools/sha256.html.

The essential thing to understand that the device ID has to be in lower cases before hashing.

# FAQ

1. **When it is needed to hash the device IDs?**
   It is not mandatory to hash the device IDs. The sole purpose of hashing is to secure the data and not share raw device IDs. Clients hash device IDs purely from security reasons.
2. **How unhashed IDs looks like?**
   The unhashed device example: 00001928-4f63-4923-8ce0-a1e2c2517385. The unhashed device ID has 36 characters (32 letters and digits plus 4 dashes).
3. **The look of devices IDs depends on what? iOS or Android? Something else?**
   There are two types of device identifiers - GAID and IDFA. Let's dig into them accordingly:
   **Google Advertising ID** — aka GAID, aka Android ID, aka Android Advertising ID (AAID) — is a device unique identifier that enables app developers and marketers to measure campaign performance and user behavior across media sources, without compromising user privacy.
   **The Identifier for Advertisers** (IDFA) is a random device identifier assigned by Apple to a user's device. Advertisers use this to track data so they can deliver customized advertising. The IDFA is used for tracking and identifying a user (without revealing personal information).
4. **Is it possible to hash device Ids ourself?**
   Yes, there are many online tools that helped to do that. For example: https://emn178.github.io/online-tools/sha256.html
5. **Are we able to get traffic for device IDs targeting from every exchange? Or only several exchanges support matches?**

The traffic with device ID will come from any exchange that has app traffic and send device ID as an identifier.

**Why do iOS device ID lists match fewer users?**

On iOS the IDFA is shared only when the user allows tracking (App Tracking Transparency, since iOS 14.5), so iOS match rates are typically much lower than Android.

---

Revision #21
Created 25 June 2021 14:37:59 by Gabriele
Updated 8 November 2026 19:27:49 by Roberta Karpoviciute