

This pdf is generated on May 9, 2024. Go to [the documentation page](#) for the most up-to-date version.

## Advanced robot blocking

By default, we block robots based on their user agent and some traces they leave in the browser by default. For most robots, this works great, but some slip through the cracks. We added *advanced robot blocking* to prevent those robots from polluting your data.

It works by having an extensive list of known IPs of data centers (from Udger, Google Cloud, Amazon AWS, Microsoft Azure). This list does not contain the IPs of your visitors. Before we store a data point, we check if the IP matches this list of IPs of data centers. If it does, we tag the datapoint as being from a robot. We never store (not even a hashed version of) the IPs of your visitors.

Advanced robot blocking settings works for all of your websites in your account.

Here is how it looks in your account settings when it's enabled:

BETA

### Advanced robot blocking

We block robots based on their user agent and some traces they leave in the browser by default. For most robots, this works great, but some slip through the cracks. We added advanced robot blocking to prevent those robots from polluting your data.

It works by having an extensive list of known IPs of robots (from [udger](#)). This list does not contain the IPs of your visitors. Before we store a data point, we check if the IP matches this list of robots. If it does, we tag the datapoint as being from a robot. **We never store** (a hashed version of) **the IPs of your visitors**.

Advanced robot blocking is **enabled** for all websites in your account.

Disable

Go to [your account](#) to enable *Advanced robot blocking*.

This pdf is generated on May 9, 2024. Go to [the documentation page](#) for the most up-to-date version.