

With the ever-increasing digital marketing and online tracking, privacy-conscious users like me seek ways to protect their digital footprints. So, Apple has rescued us with an enhanced privacy feature called Advanced Tracking Protection on iPhone, iPad, and Mac.



Now, Safari will automatically remove tracking parameters from any URL you visit. Therefore, you can enjoy a more private and secure browsing experience. Here, I will share the nitty-gritty of Advanced Tracking Protection and how it removes tracking parameters from URLs on your iPhone and Mac.

Table of Contents

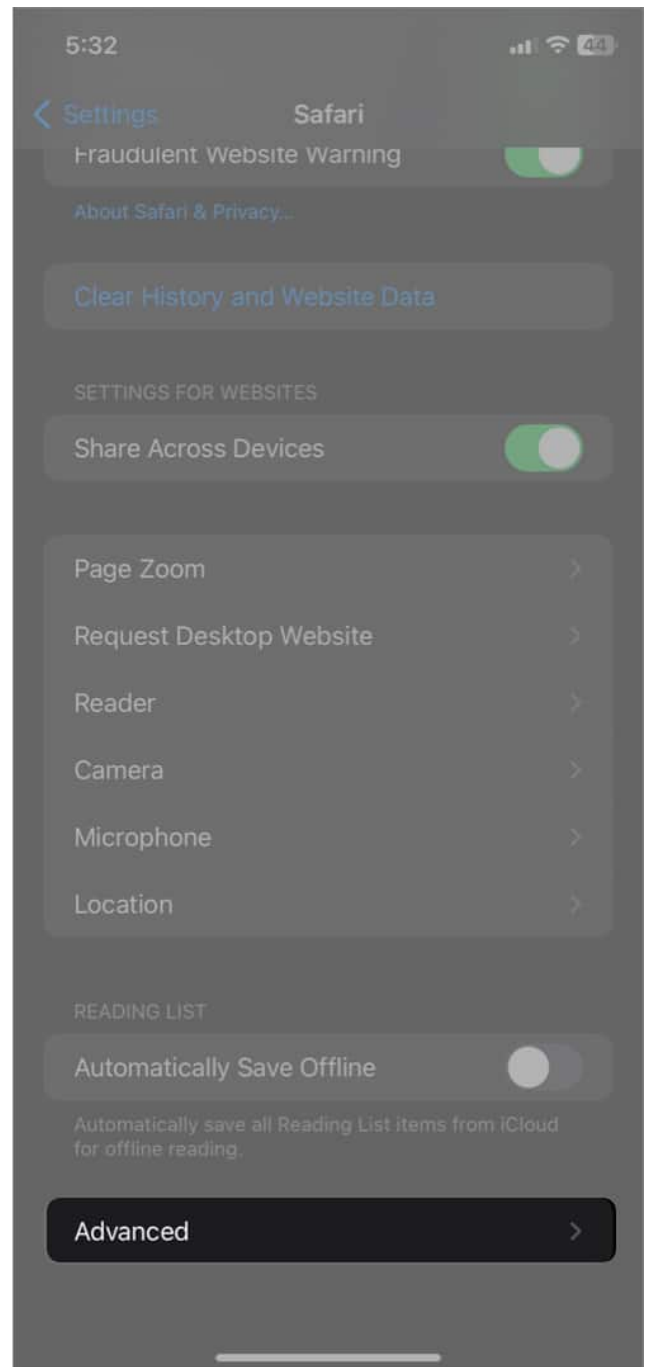
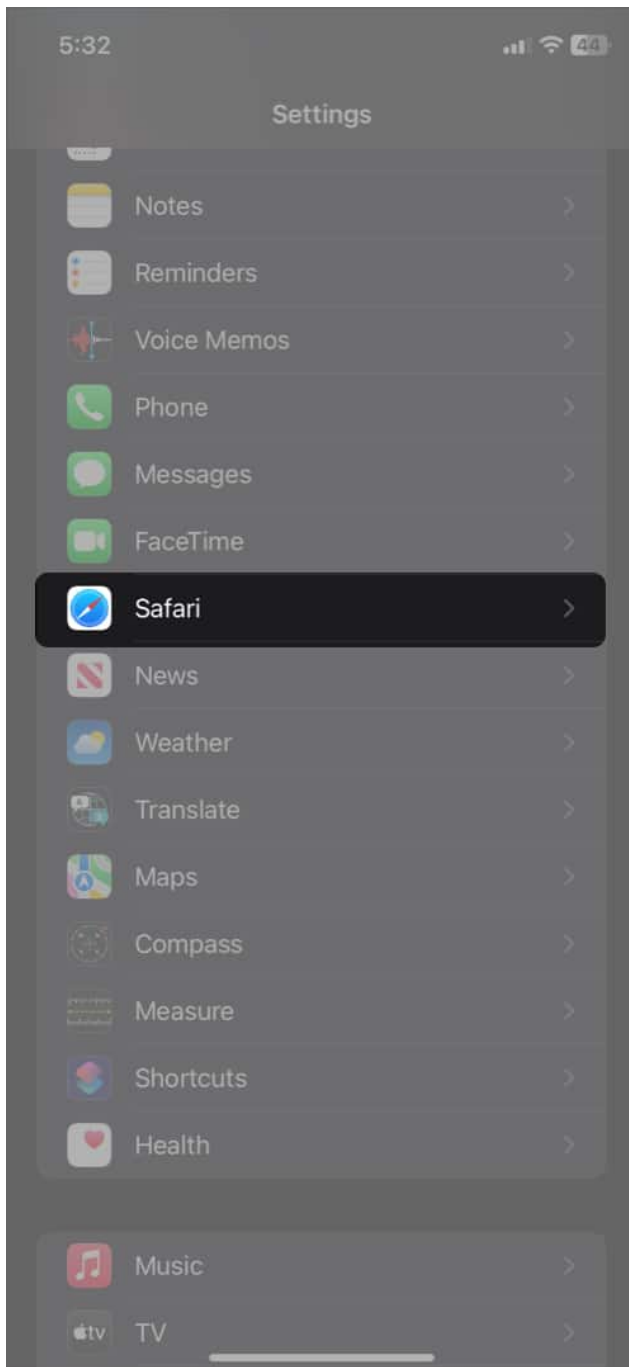
- [Enable automatic removal of tracking parameters from URL in Safari](#)
 - [On iPhone](#)
 - [On Mac](#)
- [How does Advanced Tracking Protection work on iPhone and Mac](#)
 - [How are tracking parameters identified](#)
- [Benefits of Advanced Tracking Protection](#)

Enable automatic removal of tracking parameters from URL in Safari

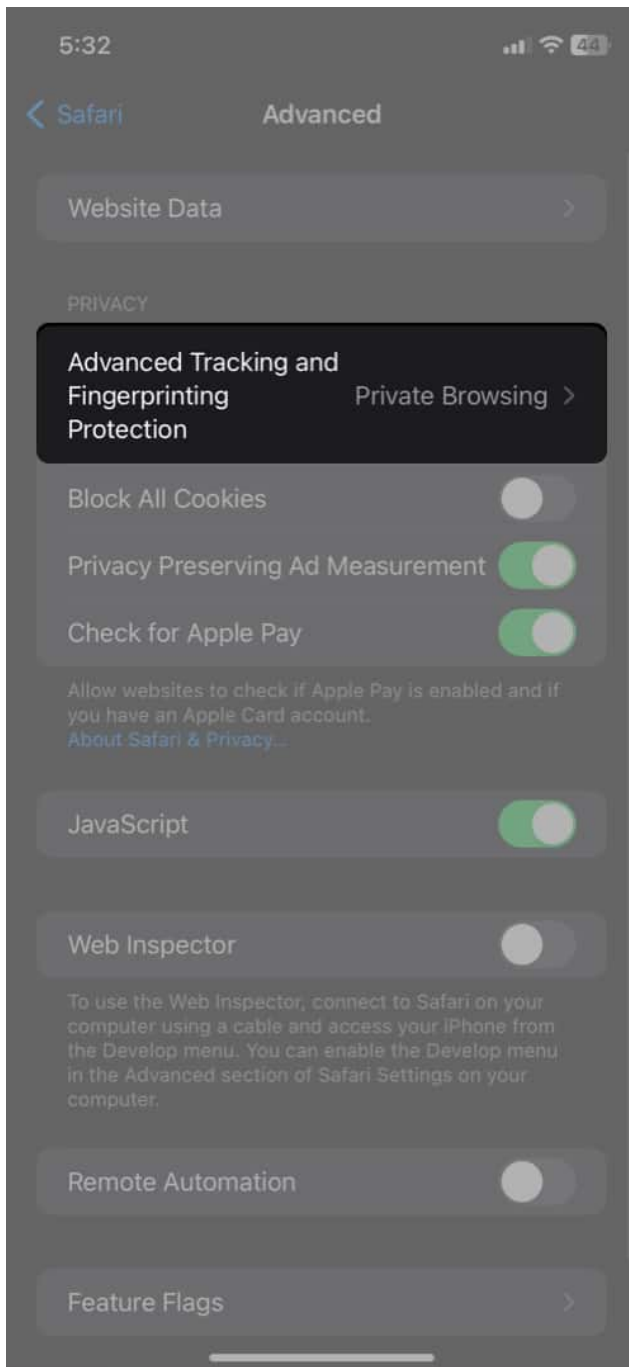
Advanced Tracking and Fingerprinting Protection is enabled for Private Browsing across all your Apple devices by default. To use it system-wide for Safari, Mail, and Messages, do the following.

On iPhone

1. Go to **Settings** → **Safari** → **Advanced**.



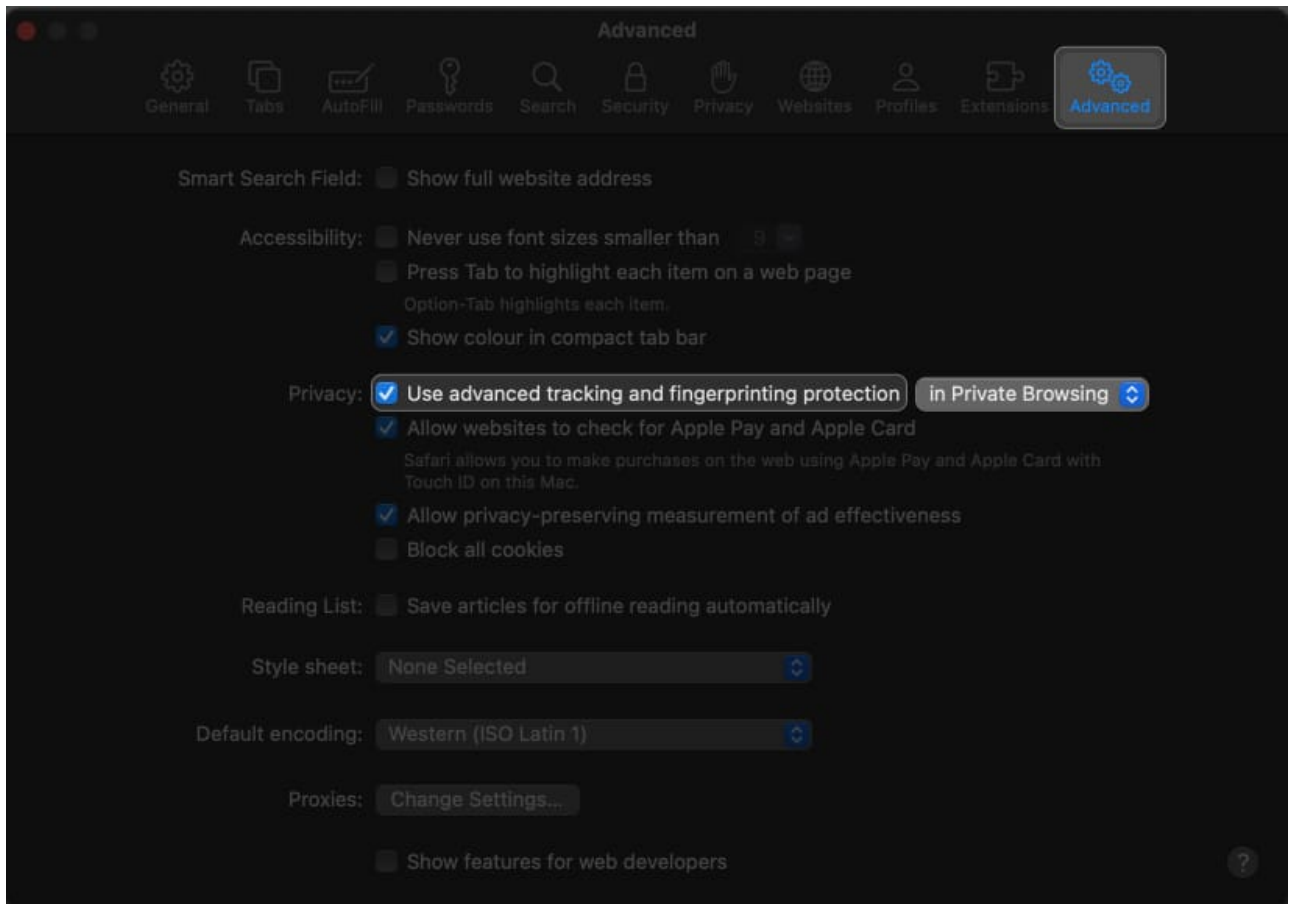
2. Tap **Advanced Tracking and Fingerprinting Protection**.
3. Select **All Browsing**.



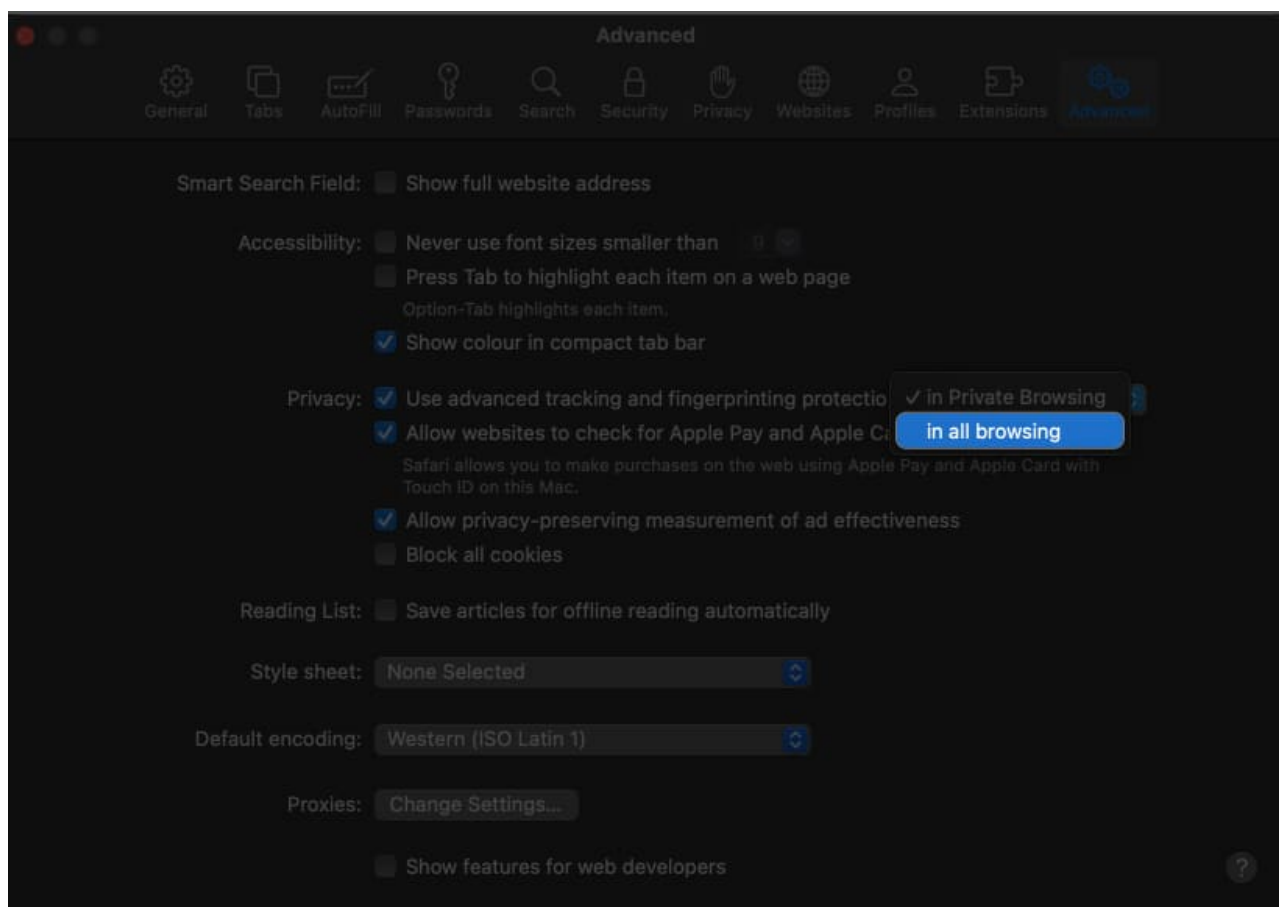
On Mac

1. Launch **Safari** on your Mac.
2. With the Safari window active, click **Safari** in the menu bar.
3. Select **Settings** → Head to the **Advanced** tab.

4. Check **Use advanced tracking and fingerprinting protection**.



5. Click the **drop-down menu** next to the aforementioned feature → Select **in all browsing**.



How does Advanced Tracking Protection work on iPhone and Mac

The Enhanced Private Browsing feature first included Link Protection. It completely blocks known trackers from loading on web pages and removes tracking parameters from URLs you visit. Also, if you copy a link with trackers, Safari strips the identifying information from the URL.

In essence, it safeguards your sensitive information and your device's identity. But keeping its vitality in mind, Apple extended the feature for all your browsing activities on Safari. It also works for the links you receive on the Messages and Mail app.

During a WWDC 2023 developer video session, Apple demonstrated how the Advanced Tracking and Fingerprinting Protection feature removes URL parameters without refreshing the page. Now you may be wondering what tracking parameters are.

How are tracking parameters identified

Tracking parameters are additional information appended to a URL's end. Websites and advertisers use these to track user behavior and gather data for analytics, advertising, or personalization. It shows how users arrived at their site, which marketing campaigns drive traffic, etc.

For example, consider the following URL:

```
https://example.com/page?click_id=Tsdht234Xser&source=advertising&campaign=summer_sale&utm_medium=email
```

In this URL, the tracking parameters are:

- **click_id= Tsdht234Xser:** It is the unique identifier assigned to the click.
- **source=advertising:** It indicates the source of the visitor, in this case, advertising.
- **campaign=summer_sale:** It identifies the specific marketing campaign associated with the URL.
- **utm_medium=email:** It denotes the medium through which the URL was shared, in this case, via email.

So, tracking parameters raises privacy concerns as it profiles individuals' online activities. Therefore, Advanced Tracking Protection in Safari helps users maintain their privacy and limit the information they share. It automatically removes the click_id and other user identifiers to avoid cross-website tracking and helps you get rid of targeted ads.

Benefits of Advanced Tracking Protection

Enabling the Advanced Tracking Protection feature for all your browsing activity offers several benefits, such as:

- **Enhanced privacy:** By removing tracking parameters from URLs, Safari helps prevent websites and advertisers from tracking your online activities. So, this makes it harder for them to create detailed profiles of your browsing habits and target you with personalized ads.
- **Improved security:** Malicious actors can potentially exploit URL tracking parameters to gather sensitive information. Thus removing these parameters reduces the risk of exposure to such threats, ensuring a safer browsing experience.
- **Faster loading times:** Many tracking parameters are used to collect data about your preferences, which can slow down website loading times. By removing them, Safari

can streamline the browsing experience and help websites load more quickly.

- **Simplified URLs:** URLs containing numerous tracking parameters can appear long and convoluted. That's why Advanced Tracking Protection presents cleaner and more readable URLs, making them easier to understand and share.

No more prying eyes!

The Advanced Tracking Protection feature in Safari on iOS 17, iPadOS 17, and macOS Sonoma protects your privacy and enhances your web browsing. It lets you enjoy a more private, secure, and streamlined online experience on your Apple devices. With the power of Link Protection, you can [erase your digital footprints](#) and enjoy online browsing without any worry.

Explore more...

- [How to lock Safari private tabs in iOS 17 and macOS Sonoma](#)
- [How to create Safari profiles in iOS 17 and macOS Sonoma](#)
- [How to hide IP address in Safari on iPhone, iPad, and Mac](#)
- [30 Best macOS Sonoma hidden features you should know!](#)