[GA4] Set up Analytics for a website and/or app

Discover how to set up Google Analytics for your website or app by creating a Google Analytics 4 property, adding a data stream, and adding your Google Analytics code.

Do you have multiple websites and/or apps? Learn how to structure your Analytics account.

Create an Analytics account

Your first step is to set up an Analytics account, unless you already have one. Skip to creating a property unless you want to create a separate account for this website and/or app. For example, you might want to create another account if this website and/or app belong(s) to a separate business.

1. Go to https://analytics.google.com.
2. In **Admin**, click **Create**, then select **Account**.
3. Provide an account name. Configure the data-sharing settings to control which data you share with Google.
4. Click **Next** to add the first property to the account.

Create a new Google Analytics 4 property

You need the Editor role to add properties to a Google Analytics account. If you created this account, you automatically have the Editor role.

You can add up to 2,000 properties (any combination of Universal Analytics and Google Analytics 4 properties) to an Analytics account. To raise this limit, contact your support representative.

To create a property:

1. Are you continuing from "Create an Analytics account", above? If so, skip to step 2. Otherwise, in **Admin**, click **Create**, then select **Property**.
2. Enter a name for the property (e.g. "My Business, inc website") and select the reporting time zone and currency. If a visitor comes to your website on a Tuesday in their time zone, but it's Monday in your time zone, the visit is recorded as having occurred on Monday.
   - If you choose a time zone that honors Daylight Savings Time, Analytics automatically adjusts for time changes. Use Greenwich Mean Time if you don't want to adjust for Daylight Savings Time.
   - Changing the time zone only affects data going forward. If you change the time zone for an existing property, you may see a flat spot or a spike in your data, caused by the time shift forwards or backwards, respectively. Report data may refer to the old time zone for a short period after you update your settings, until Analytics servers have processed the change.
   - We recommend that you change the time zone for a property no more than once per day so Analytics can process the change.
3. Click **Next**. Select your industry category and business size.
4. Click **Next**. Select how you intend to use Google Analytics.
   - Google Analytics tailors the set of default reports based on the information you provide about how you intend to use Analytics. For example, if you choose "Generate more leads," you will see a collection of reports to help you measure lead generation. Learn more about the business objectives reports collection.
5. Click **Create** and (if you are setting up a new account) accept the Analytics Terms of Service and the Data Processing Amendment.
6. Continue to Add a data stream to start collecting data.

Add a data stream

1. Are you continuing from "Create a property", above? If so, skip to step 2. Otherwise,
   a. In **Admin**, under *Data collection and modification*, click **Data Streams.**
   b. Click **Add stream**.
2. Click **iOS app**, **Android app**, or **Web**.

iOS app or Android app

When you add an app data stream, Analytics creates a corresponding Firebase project and app data stream, and automatically links the Firebase project to your property if your project and property are not already linked.

You can link to an existing Firebase project, however you have to do this from Firebase (and for a GA4 property that is not yet linked with Firebase.) Learn how.

1. Enter the iOS bundle ID or Android package name, the app name, and for iOS, the App Store ID, then click **Register app**.
2. Click **Next** and follow the instructions to download the config file for your app.
3. Click **Next** and follow the instructions to add the Google Analytics for Firebase SDK to your app.
4. Click **Next**.
5. Run your app to verify installation of the SDK and that the app is communicating with Google servers.
6. Click **Finish**. (Alternatively, click **Skip this step** if you want to complete app setup at a later time.)

Web

1. Enter the URL of your primary website, e.g., "example.com", and a Stream name, e.g. "Example, Inc. (web stream)".
2. You have the option to enable or disable enhanced measurement. Enhanced measurement automatically collects page views and other events. Once the data stream has been created, you can always go back and individually disable the enhanced measurement events you don't want to collect. So, we recommend that you enable enhanced measurement now.
3. Click **Create stream**.

Watch a step-by-step video to see how to set up Google Analytics on your website using Google Tag Manager.

Set up data collection for websites

To begin seeing data in your new Google Analytics 4 property, you'll need to do one of the following:

Add the tag to a website builder or CMS-hosted website (e.g., HubSpot, Shopify, etc.)

See if your CMS lets you enter just your Google tag ID

Many CMSs have native integrations with Google Analytics 4. If you're using one of the CMSs listed below, follow the instructions to find your Google tag ID and paste it into the Google Analytics field that your CMS provides.

To find your Google tag ("G-") ID:

1. In Google Analytics, click **Admin**.
2. **Make sure you are in the correct account and property**.
3. In the *Property* column, click **Data streams**.
4. Click the data stream for which you need the ID.
5. In the *Google tag* section, click **Configure tag settings**.
6. In the *Your Google tag* section, copy the ID that starts with "G-" or "AW-".

Enter your Google tag ID into the field that your CMS provides:

- Blogger instructions
- Drupal instructions
- Duda instructions
- GoDaddy instructions
- Google Sites instructions
- HubSpot instructions
- Magento instructions
- MonsterInsights plugin (WordPress) instructions
- One.com instructions
- Shopify instructions
- Site Kit (WordPress plugin) instructions
- Squarespace instructions
- Typo3 instructions
- Wix instructions
- WooCommerce instructions

All other website builders

If you are using a CMS or website builder that doesn't provide a field to enter your Google tag ID, you'll need to paste your Google tag into your website using your CMS's custom HTML feature.

1. Sign in to your Google Analytics account.
2. Click **Admin**.
3. At the top of the *Property* column, select your property.
4. In the *Property* column, click **Data streams > Web**.
5. Click the data stream for your website.
6. Under *Google tag*, click **View tag instructions**.
7. On the *Installation instructions* page, select **Install manually**:
   - On the screen, you'll see the JavaScript snippet for your account's Google tag. Your Google tag is the entire section of code that appears, beginning with:

```
<!-- Google tag (gtag.js) -->
```

and ending with

```
</script>
```

Paste your Google tag tag to your website using your CMS's custom HTML feature. Follow your CMS's instructions on how to do this below:

- Cart.com: Contact Cart.com support for instructions.
- PrestaShop: Contact PrestaShop support for instructions.
- Salesforce (Demandware): Contact Salesforce support for instructions.
- VTEX: Contact VTEX support for instructions.
- Weebly instructions

Data collection may take up to 30 minutes to begin. You can then use the Realtime report to verify that you're receiving data.

Add the Google tag directly to your web pages

You need access to the HTML for your web pages. Ask your web developer to perform these steps if you're unable to complete the steps yourself.

1. Sign in to your Google Analytics account.
2. Click **Admin**.
3. At the top of the *Property* column, select your property.
4. In the *Property* column, click **Data streams > Web**.
5. Click the data stream for your website.
6. Under *Google tag*, click **View tag instructions**.
7. On the *Installation instructions* page, select **Install manually**:
   - On the screen, you'll see the JavaScript snippet for your account's Google tag. Your Google tag is the entire section of code that appears, beginning with:

```
<!-- Google tag (gtag.js) -->
```

and ending with

```
</script>
```

Paste your Google tag immediately after the `<head>` on each page of your website.

Data collection may take up to 30 minutes to begin. You can then use the Realtime report to verify that you're receiving data.

*Don't see a Data Streams option in the Property column? You are in a Universal Analytics property instead of the GA4 property that you just created. Use the **property selector** or **Admin** to navigate to your new GA4 property.*

Add your tag using Google Tag Manager

For basic data collection, follow the Google Tag Manager help center instructions to add the *Google Analytics: GA4 Configuration* tag.

Next steps

After you have set up data collection, complete additional configurations to get more useful data out of Analytics. Review the checklist to learn which configurations are right for you to collect more data, filter unwanted data, and power advertising.

Give feedback about this article

Was this helpful? Yes No

Set up Analytics
- [GA4] Set up Analytics for a website and/or app
- [GA4] Configure your GA4 property using Setup Assistant
- [GA4] Set up Analytics for a CMS-hosted website
- [GA4] Add a Google Analytics 4 property (to a site that already has Analytics)
- [GA4] Set up data collection for an app
- [GA4] Get more useful data out of Analytics
- [GA4] Set up cross-domain measurement
- [GA4] Identify unwanted referrals
- [GA4] Data redaction
- [GA4] Filter, report on, or restrict access to data subsets
- [GA4] About connected site tags
- [GA4] URL builders: Collect campaign data with custom URLs
- [GA4] Set custom campaign data
- [GA4] Find your Google tag ID
- [GA4] Accelerated Mobile Pages (AMP)
- The Google tag
- [GA4] Filter incoming data

Need more help?
Try these next steps:
Post to the help community
Get answers from community members
Contact us
Tell us more and we'll help you get there

Understanding PII in Google's contracts and policies

Many contracts, terms of service, and policies for Google's advertising and measurement products refer to "Personally Identifiable Information" (PII). This is a different categorization of data from what the EU General Data Protection Regulation (GDPR) refers to as "personal data".

Please note that data excluded from Google's interpretation of PII may still be considered personal data under the GDPR, or personal information under any of the several laws that establish various rights for applicable US-state residents, and may therefore be subject to these laws.

This article explains how Google will interpret the term PII in the event PII isn't defined in your existing contract or the applicable product's terms of service or policies. This is to minimize confusion among customers and distinguish PII from concepts of personal data or personal information under the GDPR, CPRA and other privacy legislation.

What Google considers PII

Google interprets PII as information that could be used on its own to directly identify, contact, or precisely locate an individual. This **includes**:

- email addresses
- mailing addresses
- phone numbers
- precise locations (such as GPS coordinates - but see the note below)
- full names or usernames

For example, if you're a publisher whose contract prohibits you from passing PII to Google, the URLs of pages on your website that display ads by Google must not include email addresses, because those URLs would be passed to Google in any ad request. Google has long interpreted its PII prohibition in this way.

> Note: Certain products' help centers and policies set out the limited means by which certain forms of PII may be sent to Google. For avoidance of doubt, this article does not amend such provisions. So, for example, certain products allow approximate location data to be sent to Google, provided the requirements of the applicable policies are met.

Google interprets PII to **exclude,** for example:

- pseudonymous cookie IDs
- pseudonymous advertising IDs
- IP addresses
- other pseudonymous end user identifiers

For instance, if an IP address is sent with an ad request (which will be the case with almost any ad request as a consequence of internet protocols), that transmission will not breach any prohibition on sending PII to Google.

Note that data excluded from Google's interpretation of PII may still be considered personal data or personal information under the GDPR, and other privacy legislation. This article doesn't affect any contract provisions or policies relating to personal data or personal information under those laws.

Give feedback about this article

Was this helpful? Yes No

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

Help

- Data privacy and security
- How to get support
- Analytics service status
- Supported browsers
- Available languages
- Analytics policies
- Analytics APIs
- How Google Analytics secures your web traffic
- **Understanding PII in Google's contracts and policies**
- [GA4] Data collection
- Regional data collection
- Privacy Disclosures Policy
- Google Measurement Controller-Controller Data Protection Terms
- U.S. State Privacy Laws Controller Addendum to Google Measurement Controller-Controller Data Protection Terms
- Shared Data Under Measurement Controller-Controller Data Protection Terms
- Policy Requirements for Phone Analytics
- Prepare for Apple's App Store data-disclosure requirements
- Prepare for Google Play's data disclosure requirements
- Prepare your app for Android changes
- Updates to iOS 14+ campaign measurement

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

©2024 Google - Privacy Policy - Terms of Service

English

[GA4] Get more useful data out of Analytics

A checklist for marketers and advertisers to ensure that Analytics has the crucial data you need to power business measurements

After you have set up data collection for your websites and apps, complete additional configurations to get more accurate and useful data. The more items you complete on the checklist, the more complete your GA4 data will be. Many configurations determine what data is collected in your property, so it will only be available from when you complete them. That's why it's valuable to do them as soon as possible. Most configurations can be done through the Analytics interface. The few that may require help from a developer are marked "Requires working with code."

In this article:

Collect more data
Filter unwanted data
Power advertising

Collect more data

Configurations everyone should complete

Action	Outcome
Set up key events	Measure and analyze user actions that are most important to your business.
Activate Google Signals	Enable cross-device remarketing and cross-device key events export to Google Ads.
Link to Search Console	Analyze organic search results for your website in Analytics.

Configurations to consider

Action	Consider if	Outcome
Set up ecommerce events	You sell products or services on your website or app.	Collect and measure ecommerce data. *Requires working with code.*
Link to your other data sources	You have other data sources.	Analyze data from other sources in Analytics.
Import additional data	You have other data sources that aren't available as integrations.	Analyze data from other sources in Analytics.
Send offline data to GA4 using Measurement Protocol	You have point of sale (POS) kiosks or other offline key events.	Tie online to offline behavior. *Requires working with code.*
Set up cross-domain measurement	Your business has more than one domain.	Attribute activity to a single user as they cross domains.
Measure activity across platforms with User-ID	Visitors sign in to your website or app.	Associate your own identifiers with individual users to connect their behavior across different sessions and on various devices and platforms. *Requires working with code.*
Collect campaign data with custom URLs	You run ad or email campaigns other than Google Ads. (Google Ads campaigns work best with auto-tagging.)	Use UTM parameters to identify the campaigns that refer traffic from non-Google sources.

Filter unwanted data

Configurations everyone should complete

Action	Outcome
Filter out internal traffic	Exclude internal traffic from measurement.
Filter out developer traffic	Exclude test traffic generated by developers.
Filter out bots	Exclude known bots and spider traffic. *GA4 automatically filters out bots and spiders. Unlike in Universal Analytics, you don't have to do anything to turn on this option.*

Configurations to consider

Action	Consider if	Outcome
Filter unwanted referrals	Your website gets traffic from another website that you don't want to count as a referral, for example an external payment processor.	Ensure your data includes only referrals in which you're interested.

Power advertising

Configurations everyone should complete

Action	Outcome
Link to Google Ads	See Google Ads data in Analytics, use Analytics key events to bid on Ads, and use Analytics audiences for remarketing in Ads.
Allow personalized advertising	Share your audiences and key events with Google Ads. *Personalized advertising is enabled by default when you link Analytics and Google Ads.*
Import GA4 key events to Google Ads	See Analytics key event data in Google Ads and give Google Ads Smart Bidding access to data that helps optimize bids.
Build audiences	Use audiences for reporting, advertising, and optimization (e.g., A/B tests).
Enable Analytics audiences in Google Ads	Use Analytics audiences for remarketing in Google Ads.

Configurations to consider

Action	Consider if	Outcome
Create custom channel groups	Default channel groups don't meet your needs.	Use custom rule-based categories for your website traffic as dimensions in reports, explorations, and audiences.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Try these next steps:
Post to the help community
Get answers from community members
Contact us
Tell us more and we'll help you get there

Set up Analytics
[GA4] Set up Analytics for a website and/or app
[GA4] Configure your GA4 property using Setup Assistant
[GA4] Set up Analytics for a CMS-hosted website
[GA4] Add a Google Analytics 4 property (to a site that already has Analytics)
[GA4] Set up data collection for an app
[GA4] Get more useful data out of Analytics
[GA4] Set up cross-domain measurement
[GA4] Identify unwanted referrals
[GA4] Data redaction
[GA4] Filter, report on, or restrict access to data subsets
[GA4] About connected site tags
[GA4] URL builders: Collect campaign data with custom URLs
[GA4] Set custom campaign data
[GA4] Find your Google tag ID
[GA4] Accelerated Mobile Pages (AMP)
The Google tag
[GA4] Filter incoming data

©2024 Google - Privacy Policy - Terms of Service
English

Best practices to avoid sending Personally Identifiable Information (PII)

Avoid sending PII to Google when collecting Analytics data.

To protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII). PII includes, but is not limited to, information such as email addresses, personal mobile numbers, and social security numbers. Because laws across countries and territories vary, and because Google Analytics can be used in many ways, consult an attorney if you are in doubt whether certain information might constitute PII or not.

Learn more about what Google considers PII.

When implementing Analytics on a property, follow the best practices in this article to reduce the risk of passing PII to Google.

In this article:

User IDs
Page URLs and titles
PII entered by users
Data Import
Analytics features and privacy risk
Geolocation
AdSense

User IDs

Before using User IDs, read Best practices for User-ID

Page URLs and titles

The basic Analytics page tag collects the page URL and page title of each page that is viewed. PII is often inadvertently sent in these URLs and titles. Both the URL path and parameters must be free of PII. If there is any possibility of your URLs, URL parameters, or titles containing PII, you'll need to remove it.

You can configure data redaction in Analytics to remove email addresses on a best-effort basis and to remove URL query parameters that you specify. Data redaction is configured in the Admin section of Analytics and doesn't require that you write any code. It is only available for web data streams. Learn more about Data redaction.

You can also add analytics.js code to change the URL before it gets sent to Analytics. For example, to alter the URL to "example.com/example?a=b":

```
ga('set', 'location', 'http://example.com/example?a=b');
```

See the developer reference.

Similarly, you can alter the page title before it gets sent to Analytics. For example, to change the title to "New Title":

```
ga('set', 'title', 'New Title');
```

See the developer reference.

There are additional strategies to avoid sending PII through URLs. To learn more, read Best practices to avoid sending PII in the AdSense help center.

PII entered by users

Website visitors and users sometimes enter PII into search boxes and form fields. Be sure to remove PII from user-entered information before it is sent to Analytics.

Data Import

Read the Upload data use policy before using Data Import or uploading data to Analytics.

Analytics features and privacy risk

Special care should be taken to ensure no PII such as names, social security numbers, email addresses, or any similar personal identifiers, or data that permanently identifies a particular device such as a mobile phone's unique device identifier (if such an identifier cannot be reset) is sent to Analytics when using these following features:

- User ID override
- All custom dimensions
- Campaign dimensions: *Source, Medium, Keyword, Campaign, Content*
  Be sure not to include PII in custom campaign parameters utm_source, utm_medium, utm_term, utm_campaign, and utm_content.
- Site search dimensions: *Site Search Term* and *Site Search Category*
- Event dimensions: *Event Category, Event Action, Event Label*

Geolocation

If collecting geolocation info, ensure it is not GPS or fine-grained location information, as this could lead to reasonable inference of the individual. "Fine-grained location" information for Analytics is defined as any area less than 1 square mile, including any lat/long data. In some instances, such as in the UK, zip code can map to a single residence and thus cannot be passed to Analytics.

AdSense

If you use AdSense, read and follow the Best practices to avoid sending PII in the AdSense help center.

Give feedback about this article

Was this helpful? Yes No

Data privacy and security
Safeguarding your data
Privacy controls in Google Analytics
[GA4] Data redaction
Introduction to user consent management
[GA4] Verify and update consent settings in Google Analytics
[GA4] Behavioral modeling for consent mode
Google Analytics opt-out browser add-on
[UA] IP masking in Universal Analytics
[GA4] Policy requirements for Google Analytics Advertising Features
[UA] Security and privacy in Universal Analytics
Data Processing Terms
We use our own products
Data retention
[GA4] Data-deletion requests
Data deletion requests (Universal Analytics)
ISO 27001 Certification
Google Analytics links overview
Account setup with additional privacy features
Best practices to avoid sending Personally Identifiable Information (PII)
Policy Against Fingerprints and Locally Shared Objects
Data controls in Universal Analytics
Data controls in Google Analytics 4
[GA4] EU-focused data and privacy
HIPAA and Google Analytics
Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

©2024 Google - Privacy Policy - Terms of Service

English

[GA4] Google Analytics Data Controls Guide

Rising consumer expectations and changing industry regulations have set higher standards for user privacy and data protection. This has led many businesses to revisit how they are managing data in their Google Analytics accounts.

Customers are the controllers of the data that they collect through Google Analytics. To help businesses manage this data, Analytics and Google's tagging solutions provide a variety of features and controls that allow customers to govern how data is collected, stored, and used–all of which can be adjusted at any time.

The purpose of this document is to offer a central guide to Google Analytics' data practices and controls for protecting the confidentiality and security of data (information publicly available in our Google Analytics Help Center).

This document is not legal guidance. Google does not provide legal advice to customers but shares product functionality that may help customers comply based on their own assessment of local laws and regulations.

Note: Server-side tagging with Google Tag Manager- While this document outlines options for controlling or modifying data via server-side tagging, please note that some modifications may significantly impact key use cases. Also note that app data streams and some features–such as Google signals–are not yet supported for server-side implementations of GA4. We continue to explore new options for server-side implementations.

Data Collection

Note: 360 and free versions share the same technical infrastructure and data collection principles apply to both.

Customers may customize data collection by using the following Data Controls (if you want to learn more on how Google Analytics collects Data, you can visit this page):

Features	Google Analytics support	Server-side Tagging support	Feature details

Consent Mode	Consent Mode- allows you to adjust how your Google tags behave based on the consent status of your users. Google's tags will dynamically adapt, only utilizing measurement tools for the specified purposes when consent has been given by the user. Instructions for Global site tag (gtag.js) Instructions for Google Tag Manager	Consent Mode is natively supported when using a client-side GA4 config tag to route data to your server-container. Server-side Google tags will respect the consent state captured by the client-side tag without any additional configuration server-side. Server-side Tagging supports both Basic and Advanced consent mode implementations.	When consent for ad storage or analytics storage is denied, the associated Google measurement functions deployed via global site tags (gtag.js) or Google Tag Manager will adjust their behavior accordingly. For example, when analytics_storage=denied, Google Analytics will not read or write first-party analytics cookies. When ad_storage=denied, Google Analytics will not read or write Google Ads cookies, and Google signals features will not accumulate data for this traffic.
Measurement Protocol	Measurement Protocol is a server-to-server method to send data to Google Analytics . The Measurement Protocol defines how to construct the events and how to send them to Analytics. Notably, this makes it easy to measure interactions that happen server-to-server and offline.	You can utilize Measurement Protocol by sending data to your server-container in the Measurement Protocol schema and utilizing the Measurement Protocol Client in your server-container. .	The purpose of measurement protocol in GA4 is to augment existing events collected via gtag, GTM, or the Google Analytics for Firebase SDK. Some event and parameter names are reserved for use via automatic collection and cannot be sent through the measurement protocol. So while it is possible to send events to Google Analytics solely with measurement protocol, only partial reporting may be available.

Data type	Native Analytics Data Controls	Server-Side Tagging Controls	Impact if altered or redacted
Client ID	You have control over the Client ID value that will be used by Google Analytics. • Client ID configuration field • Consent Mode allows you to adjust how your Google tags behave based on the consent	You have the control to modify or remove the Client ID value in Server-Side GTM with a Custom Variable and Sandboxed JavaScript.	If the client ID is different between the cookie value and the value used in Google Analytics (including when client ID is not present), you will not be able to use audience remarketing functionality. Modification of client ID may

	status of your users.		reduce accuracy of user/visitor counts. If client ID is removed, Analytics may begin to report on multiple users as a single user and deflate user counts. If client ID is changed, Analytics may begin to recognize a single user as multiple users and inflate user counts. Please note that the value used in Google Analytics is the one being used in case of data deletion or data portability. Google Analytics will not will not read or write first-party analytics cookies when analytics_storage=denied.
Advertising Identifiers	When Google signals are enabled (optional feature), Google Analytics collects visitation information and associates it with Google information from accounts of signed-in users who have consented to this association. For web data streams, Google Analytics collects the information it normally does, as well as Google advertising cookies when those cookies are present. For app streams, Google Analytics collects DSID for Android and identifier for advertisers (IDFA) for iOS. Controls available: • At property and regional level with Google Signals admin settings on/off toggle • At user level with gtag.js function GTM template option	*Server-side tagging does not yet support Google signals or collect advertising identifiers. There are plans to launch Google Signals support later in 2023.*	If you deactivate Google signals, Analytics stops collecting Demographics and Interests information. When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features • Cross Device reports If you deactivate Advertising Reporting Features, Analytics stops collecting Demographics and Interests information. When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features

User ID	A User ID is a unique, persistent, and non-personally identifiable ID string that represents a user. It enables the analysis of groups of sessions across devices. You must first enable it in your Analytics account and then implement it in your tracking code. You have control over the User ID value that will be used by Google Analytics. Set up User ID	User ID can be transmitted to Server-Side GTM and then utilized by your server-side GA4 tags once User ID is configured in your web container (Tag Manager and User ID). Server-Side GTM can be used to redact or modify User ID if required with a Custom Variable or with the parameters to drop/add section in the server-side GA 4 tag.	If User-ID is not collected by Analytics: • No User-ID-based reporting when Reporting Identity is set to Blended Views • If a unique identifier is not available, you may experience inflated user counts, as the same visitor on a different browser or device would be recognized and reported as a new unique user by Analytics • No cross-device or cross-platform ads personalization
Granular Location & Device	You have control over the granular location and device data that is collected about your visitors. When collection is disabled, city-level location data as well as certain device-level metadata is redacted prior to collection in Google Analytics' servers. Controls available: Disable collection at property and region level with granular location and device data collection setting	Server-side GTM supports the location and device controls as configured in your Google Analytics property. Server-side GA4 tags will automatically respect your location and device data settings.	If you deactivate granular location and device data collection, Analytics stops collecting this information and it will not be available in reporting and related Analytics features. • City • Latitude (of city) • Longitude (of city) • Browser minor version • Browser User-Agent string • Device brand • Device model • Device name • Operating system minor version • Platform minor version • Screen resolution
Referrer and **URL Parameters**	You have control over the page referrer and URL parameter values that are used by Google Analytics. • Page referrer • URL parameters	You have the control to modify or redact the referrer and UTM parameter values in Server-Side GTM with a Custom Variable and Sandboxed JavaScript.	Removal of URL parameters or referrer could impact the accuracy of conversions and traffic source attribution. For example, modification of UTM parameters could lead to misattributed traffic sources.

Transaction ID	You have control over the Transaction ID value that will be used by Google Analytics. Transaction ID field reference	Server-Side GTM can be used to redact or modify Transaction ID if required with a Custom Variable or/and with the parameters to drop/add section in the server-side GA 4 tag.	If altered, the same-session transaction ID deduplication process might not work and may result in inflated or inaccurate transaction reporting.
IP address	Location data is inferred from the visitor IP address. IP addresses are immediately discarded after location data is inferred and IP address data is never logged or stored on Analytics databases.	The GA4 server tag in Server-Side GTM allows you to redact IP addresses in your server container. If the option to redact is not selected, the IP address will automatically be masked by your GA4 server-tag.	Location data is not collected by Analytics (GA4). If you redact IP addresses using Measurement Protocol or server-side GTM, Google Analytics would not be able to automatically supply you with location data in reports. Spam and bot detection will also be impacted when IP address is not sent to Analytics from server-side GTM.
Cookie parameters	Google Analytics' cookies default behavior can be customized. For example, you can define a prefix name, restrict the cookie to a specific subdomain, set up an expiration date and disable its auto-update. Visit this dev page for more information on available Cookie parameters. Cookie parameters Google Analytics' cookie expiration period can be overridden by changing the default cookie settings.	Server-Side GTM allows you to customize Google Analytics' cookie behavior. Similar to the client-side GA4 tag, Server-Side GTM allows you to adjust the prefix name, restrict a cookie to a specific subdomain, set up an expiration date and disable auto update. Additionally, Server-Side GTM supports 'Server Managed cookies', which are only accessible via HTTP. You can read more about Cookie parameters available in Server-Side GTM on this developer page. There is also more general guidance on this Tag Manager developer page.	Altering cookies could result in less reliable attribution data.
Personally Identifiable Information (PII)	Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII). Here are some best practices to avoid sending PII.	N/A	N/A

Data Usage

Usage Control	Available Data Controls	Impacts if altered or redacted
Google signals	Google signals is an optional feature that can be enabled to provide demographics and interest data, cross-platform reporting, remarketing audiences, and ads personalization (when ads personalization is also enabled). Controls available: • At property and regional level with the Google Signals admin settings on/off toggle *Google signals are not supported for Analytics data that are sent to Analytics through Measurement Protocol or server-side tagging.	When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features • Demographics and Interests Reports • Cross Device reports
Ads Personalization	Customers may choose to disable Advertising Personalization for data collected from their entire property, or to disable it for individual events or users (for apps, websites, and measurement protocol). Controls: • Control by region • Disable advertising features (gtag.js) • Event controls in Measurement Protocol • Consent Mode	If you disable ads personalization for a given user/property/region, then all events collected from those locations will be marked as not eligible for use for ads personalization (NPA). This means that any conversions from these users will be marked as not for use for ads personalization even when exported to your linked ads accounts. In addition, any end user coming from a disabled location will not be added to any lists that may be exported to your linked ads accounts, although lists that have already been exported will not be affected. All events collected for the property, and any audiences based on that data, are still available within Analytics for use in reports, Analysis, and audience building.
Data sharing settings	Customers may choose to share their Google Analytics data for various purposes (Google Product & Services, Benchmarking, Account Specialists, Technical Support) Any data collected and used by Google under the "Google products & services" setting is subject to the Controller-Controller Data Protection terms and Google is, for GDPR purposes, an independent controller of such data. Regardless of your data sharing settings, your Analytics data may also be used only insofar as	In order to benefit from Predictive Metrics, you must enable the Modeling contributions & business insights data sharing setting.

	necessary to maintain and protect the Analytics service.	

Data Storage

Setting	Definition	Available Data Controls
Data Retention	The Google Analytics Data Retention controls give you the ability to set the amount of time before event-level data stored by Google Analytics is automatically deleted from Analytics servers. The retention period applies to user-level and event-level data associated with cookies, user-identifiers (e.g., User-ID), and advertising identifiers (e.g., DoubleClick cookies, Android's Advertising ID [AAID or AdID], Apple's Identifier for Advertisers [IDFA]).	For Google Analytics 4 properties, the setting applies to event-level data. You can choose: 2 months 14 months 26 months (360 only) 38 months (360 only) 50 months (360 only)

Data Portability

Portability Option	Available Data Controls
User-level Data Access and Portability	For Google Analytics 4 properties, you can pull event information for any given user identifier via User Explorer. This allows you to analyze and export event level data for a single user identifier.
BigQuery Export	GA4 customers can integrate with BigQuery to create a full export of all event data associated with their users to a single queryable repository.

Data Deletion

Data Erasure Option	Available Data Controls	Impacts if altered or disabled
Data Deletion Requests	If you need to delete data from the Analytics servers for any reason, then you can use the Data Deletion Requests feature to issue a request for its removal.	You can select All to delete all data for the property, or select one or more individual fields (e.g., URL*, Page Title, Event Category).
User Data Deletion	Customers may delete a single user's data from Google Analytics by passing a single user identifier	Once deletion is requested, data associated with this user identifier will be removed from the Individual User Report within 72 hours, and then deleted from Analytics

	to the Google Analytics User Deletion API or via our User Explorer report.	servers during the next deletion process. Reports based on previously aggregated data (for example, user counts in the Audience Overview report) will not be affected.

Set up enhanced conversions for leads with the Google tag

The "Linked Accounts" page under Admin has been moved to "Data manager" under Tools. Google Ads Data Manager is a data import and management tool with a point and click experience that lets you bring your customer data from outside of Google and activate it in Google Ads. Learn more About Data manager.

Note: The global site tag (gtag.js) is now the Google tag. With this change, new and existing gtag.js installations will get new capabilities to help you do more, improve data quality, and adapt new features — all without additional code. Learn more About the Google tag.

Enhanced conversions for leads uses first-party user-provided data from your website to measure sales and transactions that happen off your website. If you run lead-generation campaigns to drive offline sales, enhanced conversions for leads can help you understand the impact of your ad spend.

Enhanced conversions for leads relies on a tag to capture first-party data to enable durable, more accurate, and higher quality measurement. With enhanced conversions for leads, you can upload deeper lead data back into Google in a durable way, to further drive reporting and optimization insights.

This article explains how to use the Google tag to set up enhanced conversions for leads measurement on your website using the Google tag. If you use Google Tag Manager, view set up enhanced conversions for leads using Google Tag Manager. If you want to learn more about the benefits of enhanced conversions for leads and how they work, check out About enhanced conversions.

Note: When enhanced conversions for leads are enabled, the associated tag will automatically capture relevant form interaction events on your website.

Before you begin

Before setting up enhanced conversions for leads, you'll need to identify your website lead forms and pick a field from the form that uniquely identifies a lead. At least one of the following variables must be provided when you configure enhanced conversions for leads on your website and when you later import the conversions:

- Email (preferred)
- A phone number

We recommend using the lead's email address because it's a highly unique identifier and isn't prone to being reformatted in your CRM. If you're using a phone number, the tag will remove symbols and dashes, but the number must contain a country code.

You'll also need to:

- Note the URL where the lead form on your website is located. You may need this information during setup.
- Make sure that auto-tagging is enabled. Auto-tagging is necessary to import offline conversions.
- Make sure that there is first-party customer data available (email and/or phone number) on your website lead form.
- Ensure that you have reviewed and confirmed that you can comply with the customer data policies in Google Ads (view steps on this below).

Instructions

Note: The instructions below are part of the steps to set up Google Ads conversion measurement. To view the setup steps, click the "Appearance" icon, and select **Steps**. If you're using the previous version of Google Ads, review the Quick reference map or use the Search bar in the top navigation panel of Google Ads to find the page you're searching for.

Here's an overview of the steps for setting up offline conversion imports using enhanced conversions for leads:

1. Configure the Google tag
2. Create a new conversion action
3. Accept Customer data terms

1. Configure Google tag

1. Select how you want to set up your provided data. You can select either "Google Tag" or "Google Tag Manager" before clicking **Continue with Google click identifiers**.
   - **Google tag**: If your provided data is off, you'll receive an error message and direction to configure your tag. If your tag is configured correctly, you'll receive a success message.
   - **Google tag manager**: You'll receive a notification with links to instructions and the Google Tag Manager page.
2. Next to "Google tag configuration", click **Configure tag**.
3. In the "Your Google tag" section, ensure the Google tag is installed on your website.
4. In the "Settings" section, click the arrow for "Automatically detect events".
5. In the "Configuration" section that opens, make sure "Form interactions" is toggled on, then click **Save**.
6. In the "Settings" section, click the arrow for "Include user-provided data from your website".
7. In the "Configuration" section that opens, click "Include user-provided data from your website".
   - Select how you'd like to include user-provided data:
     - **Automatic collection**. This automatically imports the page for strings that match a pattern for email addresses. You can also click the "Exclude some CSS selectors from automatic collection" checkbox to limit automatic collection to certain pages, forms or parts of your site.
     - **Manual configuration**. Specify CSS selectors or JavaScript variables on your page.
     - **Image code**. Add JavaScript code to your website that sends an event.
   - Click **Save**.

Notes

- If your transactions are related to sensitive categories, you should use manual configuration to ensure that sensitive data isn't shared with Google.
- If you implement manual or automatic collection, your tag can include user-provided data with lead form events to simplify the import process. Configure how the user-provided data is included. Google is committed to protecting the confidentiality and security of the data you share with us. Learn more about Customer data policies.

8. In the "Google tag" menu, click **Save**.
9. You'll receive a success notification. Click **OK**.

Next, you'll need to import conversions from ad clicks into Google Ads.

2. Create a new conversion action

1. In your Google Ads account, click the **Goals** icon.
2. Click the **Conversions** drop down in the section menu.
3. Click **Summary**.
4. Click **New conversion action**.
5. Select **Import** in the "New conversion action" page.
6. Select **CRMs, files, or other data sources** and then **Track conversions from clicks**.
7. In the "Data Source" section, select **Connect a new data source**.
   a. You can choose to connect data sources via:
      i. Direct connection
      ii. Third-party integration by Zapier
8. Click **Continue**.
9. Enter the settings for this conversion action. For details on the settings, check out Set up offline conversion imports.
10. Click **Save and continue**. The next page will confirm your conversion action.

    Note: If you initially skipped connecting data sources, click **Set up** in the "Set up data sources" section.

11. Click **Done**.
12. Check the box to Turn on enhanced conversions for leads. If you don't want enhanced conversion for leads, you can click Continue with Google click identifiers or Finish setup later. If you'd like to turn it on after you've set up your conversion action, you can Click **Summary**. In the enhanced conversions for leads drop down, check the box to **Turn on enhanced conversions for leads**.

3. Accept Customer data terms

If you haven't yet accepted the Customer data terms, you can review and accept them by following these instructions:

1. Next to "Customer data terms", select **View Terms** and review the "Policies and Additional Terms for Customer Data".
2. Click the "I have read and accept the terms on behalf of my company" checkbox.
3. Click **Agree**. You'll notice your status is updated to "Accepted".

Note: These terms apply to your entire account or manager account. If you're not able to view the terms, your account conversions are tracked by a manager account. The customer data terms must be accepted from the manager's account and any Google Ads manager account uploading on behalf of the manager account using cross-account tracking.

Set up enhanced conversions for leads using Javascript or CSS selectors

If you're using Javascript variables, it's likely easiest to ask your developer which variables should be added to these fields. If you're using CSS Selectors, you can follow the steps below.

Find enhanced conversions fields on your lead form page

1. Using the Chrome browser in a separate tab from your Google Ads account, navigate to your lead form submission page.
2. Identify the fields where customer data is entered on the page that you wish to send to Google.

   Note: At least one of the following fields must be provided for enhanced conversions to work properly:
   - An email (preferred)
   - A phone number

3. Once you've identified the customer data fields on the page, you'll need to follow the next step to copy the CSS Selectors and enter those into Google Ads.

Identify enhanced conversions CSS Selectors and input into Google Ads

1. On your lead form page, when you've found the corresponding customer data you want to send, use your mouse to right-click on top of it and select **Inspect**.

   Note: If you're inputting the CSS selector for email in Google Ads, make sure you right-click the email address displayed on your lead form page.

2. You'll notice the Chrome Developer Tools launch within your Chrome browser.
3. Within the source code presented in the Chrome Developer Tools page, a portion of the code will be highlighted. This highlighted code is the portion which includes the CSS Selectors for the customer data you right-clicked in Step 2 of this section.
4. Hover your mouse over the highlighted code and right-click it.
5. Scroll down to "Copy" and then choose **Selector**.
6. Paste that text in the Google Ads automatic enhanced conversions section (on your other tab) in the corresponding field.
   - For reference, it should look something similar to but not exactly like this:
     `tsf > div:nth-child(2) > div.AfSBwf > div.RNNXgb > div > div.aMzic > centfmal`
7. Complete steps 2-6 of this section for each different customer data type (email or phone)
8. In your Google Ads account, click **Save**.

Note: It is a best practice to use the ID attribute to retrieve the value from a DOM element. IDs are unique and less likely to change over time than other properties, such as class names or names. They also aren't affected by layout changes, which means that your code will still work even if the layout of your page changes.

If a field doesn't already have an ID, you can add one by using the `id` attribute in the HTML. For example:

```
<input type="text" id="myTextField">
```

Set up enhanced conversions for leads by editing your website code

You can implement enhanced conversions for leads with custom Javascript code to call the Google tag, directly (forms hosted by a third party tool or iFrame may require this) instead of automatic detection or through selectors.

Identify and define your enhanced conversions fields

Ensure your email or phone number are available to your custom code. You can either send unhashed data, which Google will normalize and hash before the data reaches the servers, or normalized and hashed data. If you decide to normalize and hash the data, follow the below instructions.

For normalization:

- Remove leading and trailing whitespaces.
- Convert the text to lowercase.
- Format phone numbers according to the E.164 standard.

For hash:

- Use hex **SHA256**.

The table below lists more information about the fields you can define. The "Key Name" column indicates how they'll be referenced in the enhanced conversions HTML snippet, which is created in the next step. Note, all data should be passed as String types.

Data Field	Key Name	Description
Email address	`email`	User email. Example: `jdoe@example.com`
	`sha256_email_address`	Hashed user email. Example: `1a8af3a9f99b3d2f2ca6e0e5a6d5d4fc157439c38b28da5`
Phone number	`phone_number`	User phone number. Must be in E.164 format, which near-15 digits including a plus sign (+) prefix and country code w/ parentheses, or spaces. Example: `+1(212)345678`
	`sha256_phone_number`	Hashed user phone number. Example: `1e92ba4fc77f4a35cf8020f10b74b0e53d64cac4cea6004e5f95f`

Note: You'll need to make sure the customer data is available when the custom code fires. If the user information is collected on a previous page or iframe, you'll need to make sure it's available in a variable to your code when it's called.

Implement the enhanced conversions script

Configure and add the following script to where you want the Google tag to fire. Ensure you update variable names below to match the variable names for those attributes on your web page.

For example, if you store email in a variable named `"email_address"` then the snippet should be edited to reflect that (for example, where it says yourEmailVariable)

Note: You can also hardcode the field with a string or use a function instead of using variables.

```
// Implement the user-provided data object
<script>
gtag('set', 'user_data', {
"email": yourEmailVariable, /**Change yourEmailVariable to the actual Javascript variable name where you are storing the user's email data. Do the same for the other variables below. Make sure the values aren't hashed.
"phone_number": yourPhoneVariable, /**The phone number must be in E.164 format, which means it must be 31-15 digits including a plus sign (+) prefix and country code with no dashes, parentheses, or spaces.
});
</script>
// Send the user-provided data using the following code snippet
<script>
gtag('event', 'form_submit', {'send_to': 'AW-ID'}); /**Keep for- as is and change ID to your Google tag ID.
</script>
```

If your site doesn't collect one of the above fields, remove the field entirely rather than leaving it blank. For example, a website that only collects emails would look like this:

```
// Implement
<script>
gtag('set', 'user_data', {
"email": {{ yourEmailVariable }}
});
</script>
```

Multiple values

Developers can optionally provide multiple values (up to 3 for phone and email and 2 for address) by using an array value rather than a string. If you capture more than one value, providing this will increase the likelihood of a match. Check the example below:

```
<script>
gtag('set', 'user_data', {
"email": [yourEmailVariable1, yourEmailVariable2],
"phone_number": [yourPhoneVariable1, yourPhoneVariable2]
});
</script>
```

Example code for providing pre-hashed user data would look like this:

```
// Implement
<script>
gtag('set', 'user_data', {
"sha256_email_address": [{ yourEmailVariable }],
"sha256_phone_number": [{ yourPhoneVariable }]
});
</script>
```

Related links

- About offline conversion imports
- About enhanced conversions
- Set up offline conversion imports

Give feedback about this article

Enhanced conversions
About enhanced conversions
Set up enhanced conversions for leads with the Google tag
Set up enhanced conversions for leads with Google Tag Manager
Enhanced conversions for web impact results
About the enhanced conversions for web Ads API diagnostics report
Set up conversion-based customer lists
Set up enhanced conversions for web using Google Tag Manager
Set up enhanced conversions for web using the Google tag
Upgrade offline conversion import to enhanced conversion for leads

Achieve your advertising goals today!
Attend our Performance Max Masterclass, a livestream workshop session bringing together industry and Google Ads Pillar experts.
Register now

Safeguarding your data

Laws protecting user privacy such as the European Economic Area's General Data Protection Regulation and other privacy laws that establish various rights for applicable US-state residents impact content publishers, application developers, website visitors, and application users. See also the Google privacy policy and Google's site for customers and partners. Currently such regulations apply to specific geographic regions, but publishers and application developers often implement controls that affect the experience of users in all regions.

Google is committed to protecting data confidentiality and security. It is important to understand your privacy options, whether in the role of a publisher or a consumer. This page provides information on data collection and security for:

- Content publishers and app developers ("customers") using Google measurement products.
- Website visitors and app users ("users") of sites and apps using Google measurement products.

Data collection

Google customers use tags on web pages and an SDK for mobile apps to enable Google measurement products. The measurement data collected helps customers understand their users' needs and, optionally, personalize the user experience and offer relevant advertising (see Advertising personalization).

Google tags and the SDK use cookies and app instance IDs, respectively, to measure user interaction. While these identifiers provide information about user behavior, Google prohibits customers from sending Personally Identifiable Information to Google Analytics. Even so, use of cookies and app IDs falls under the privacy laws mentioned previously. Google customers need to inform users about the information being stored and give them the opportunity to grant or deny their consent.

See the following sections on this page to:

- Learn how Google collects and processes information about website and app usage: Information for sites and apps using Google Analytics.
- Learn about our user policies and controls: Information for visitors of sites and apps using Google Analytics.
- Download this diagram that explains how Google Analytics collects, filters, and stores data.

Information for visitors of sites and apps Using Google Analytics

Our privacy policy

At Google, we are keenly aware of the trust you place in us and our responsibility to keep your privacy and data secure. As part of this responsibility, we let you know what information we collect when you use our products and services, why we collect it, and how we use it to improve your experience. The Google privacy policy & principles describes how we treat personal information when you use Google's products and services, including Google Analytics.

Google Analytics cookies and identifiers

Google Analytics mainly uses first-party cookies to report on visitor (aka. user) interactions on Google Analytics customers' websites. Users may disable cookies or delete any individual cookie. Learn more

In addition, Google Analytics supports an optional browser add-on that - once installed and enabled - disables measurement by Google Analytics for any site a user visits. Note that this add-on only disables Google Analytics measurement.

Where a site or app uses Google Analytics for Apps or the Google Analytics for Firebase SDKs, Google Analytics collects an app-instance identifier — a randomly generated number that identifies a unique installation of an App. Whenever a user resets their Advertising Identifier (Advertising ID on Android, and ID for Advertisers on iOS), the app-instance identifier is also reset.

Where sites or apps have implemented Google Analytics with other Google Advertising products, like Google Ads, additional advertising identifiers may be collected. Users can opt-out of this feature and manage their settings for this cookie using the Ads Settings. Learn more

Information for sites and apps using Google Analytics

Google Analytics under the General Data Protection Regulation (GDPR)

Google operates as a data processor for Google Analytics. This is reflected in our Ads Data Processing Terms, which are available to all Google Analytics customers with direct contracts with Google. Learn more

Google Analytics is a data processor under GDPR because Google Analytics collects and processes data on behalf of our clients, pursuant to their instructions. Our customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time. Google's use of data is controlled by the terms of its contract with Google Analytics customers and any settings enabled by customers through the user interface of our product.

Google Analytics under privacy laws in the United States

In order to help Google Analytics customers prepare for laws that establish various rights for applicable US-state residents, we have updated our Data Processing Terms to include a *U.S. State Privacy Laws Service Provider and Processor Addendum*. Subject to the full terms of this addendum, Google Analytics will act as a service provider to its customers (when data sharing with Google products and services is disabled) and as such, will only use data collected on behalf of the customer in Google Analytics to provide the Google Analytics services. Customers who have not accepted our Data Processing Terms can do so per these instructions. Customers who have already accepted our Data Processing Terms will not need to take additional action to accept the CCPA service provider addendum. Customers should review the *U.S. State Privacy Laws Service Provider and Processor Addendum*, as well as Google Analytics' use of data, to ensure it meets customer's compliance needs.

To help customers manage their compliance needs, Google Analytics offers a collection of tools, detailed below, that enable you to control how data is collected, and whether it is used for advertising personalization.

If you have linked Google Analytics to another product, please refer to Google Analytics linking overview.

Google Analytics under the Lei Geral de Proteção de Dados (LGPD)

Google operates as a data processor for Google Analytics. This is reflected in our Ads Data Processing Terms, which are available to all Google Analytics customers with direct contracts with Google. Learn more

Google Analytics is a data processor under LGPD because Google Analytics collects and processes data on behalf of our clients, pursuant to their instructions. Our customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time. Google's use of data is controlled by the terms of its contract with Google Analytics customers and any settings enabled by customers through the user interface of our product.

International transfers

See here for information on data transfers via Google Analytics.

Data Collected by Google Analytics

First-party cookies

Google Analytics collects first-party cookies, data related to the device/browser, IP address (when collecting data, Google Analytics 4 does not log or store IP addresses), and on-site/app activities to measure and report statistics about user interactions on the websites and/or apps that use Google Analytics. Customers may customize cookies and the data collected with features like cookie settings, User-ID, Data Import, and Measurement Protocol. Learn more

Google Analytics customers who have for instance, enabled the analytics.js or ga(.)js collection method can control whether or not they use cookies to store a pseudonymous or random client identifier. If the customer decides to set a cookie, the information stored in the local first-party cookie is reduced to a random identifier (e.g., 12345.67890).

For customers who use the Google Analytics for Apps SDK, we collect an App Instance Identifier, which is a number that is randomly generated when the user installs an app for the first time.

Advertising identifiers

Where customers use Google Analytics Advertising Features, Google advertising cookies are collected and used to enable features like Remarketing on the Google Display Network. These features are subject to the users' Ads Settings, the Policy requirements for Google Analytics Advertising Features and Google's EU User Consent policy, which requires customers to obtain consent for cookies where legally required—including consent for personalized ads. For more information about how Google uses advertising cookies, visit the Google Advertising Privacy FAQ. It is possible to implement Google Analytics without affecting normal data collection where Advertising features are disabled until consent is obtained (see Privacy Controls in Google Analytics), as well as prevent certain data from being used for advertising personalization purposes (See Advertising Personalization below).

PII prohibition

Our contracts prohibit customers from sending Personally Identifiable Information to Google Analytics. Customers should follow these Best Practices to ensure PII is not sent to Google Analytics.

What is the data used for?

Google uses Google Analytics data to provide the Google Analytics measurement service to customers. Identifiers such as cookies and app instance IDs are used to measure user interactions with a customer's sites and/or apps, while IP addresses are used to provide and protect the security of the service, and to give the customer a sense of where in the world their users come from. Customers may also choose to use the data collected by Google Analytics for sitelange personalization or advertising purposes, including ads personalization (See Advertising Personalization below).

Data access

We do not share Google Analytics data without the customer's authorization (including via settings in the product user interface), or as otherwise expressly permitted under the terms of their Google Analytics agreement, except in limited circumstances when required by law.

Customers may control their own access to data in their Analytics accounts or properties by configuring view and edit permissions for employees or other representatives who may login to their Analytics account. Learn more

Security-dedicated engineering teams at Google guard against external threats to data. Internal access to data (e.g., by employees) is limited by strict access controls (both internal policy controls and automated technical controls such as authentication, SSL, and security logs) to only those with a business need to access it.

Product linking summary

Where customers link their Analytics property to another Google product or service account ("Integration Partner"), certain data from that Analytics property may be accessed and exported into the linked account. Once data is exported through a linking integration, it becomes subject to the Integration Partner's terms and policies.

Note that once data is sent to an Integration Partner, that the data sent is subject to the terms of that Integration Partner and that Google Analytics no longer maintains access or control over that data.

Customers may review and manage their product integration linkings at any time within the Analytics product linking summary user interface.

Data sharing

Google Analytics provides several data sharing settings to customers, through which customers may customize how data collected using an Analytics data collection method (like the JavaScript code, mobile SDKs, and the Measurement Protocol) may be accessed and used by Google according to customer preferences. Note that these settings only apply to data collected from websites, mobile apps, and other digital devices using Analytics; they do not apply to data relating to a customer's use of Analytics such as the number of properties and which additional features are configured. Regardless of a customer's data sharing settings, Analytics data may also be used only insofar as necessary to maintain and protect the Analytics service. Learn more

Data Controls for retention, deletion, and portability

Data retention

With the Data Retention controls, customers can limit or expand the duration for which their user-level and event-level data is stored in Google Analytics servers. All customers should review their Data Retention settings and ensure the appropriate retention is selected.

User deletion

Customers may delete a single user's data from Google Analytics by passing a single user identifier to the Google Analytics User Deletion API or via our User Explorer report. However, this does not delete aggregate data associated with that user, such as page URLs visited.

User-level data access and portability

Customers may pull event information for any given user identifier via our User Explorer report or the User Activity API. These features enable customers to analyze and export event level data for a single user identifier. In addition, our 360 customers may integrate with BigQuery to create a full export of all event data associated with their users in a single queryable repository.

Advertising personalization

Customers may choose to limit use of their analytics data for advertising personalization purposes, instead of disabling the collection of all analytics data or advertising identifiers (see "Privacy Controls in Google Analytics"). Customers may choose to disable Advertising Personalization for data collected from their entire property, or to disable it for individual events or users (for apps, websites, and measurement protocol). Customers using Google Analytics for Firebase or Google Analytics 4 properties may also exclude specific events or user properties (like 'purchase' or 'gender') from being used for Ads Personalization.

If any of 1) all property-level data, 2) individual events, or 3) specific event names or user properties have been excluded from ads personalization, then Analytics will append an additional signal (called 'npa') in Postbacks indicating that networks should not use the data for personalized advertising. Note that each network's treatment of such 'npa' signal is determined by such network.

Data privacy and security

Certifications

ISO 27001

Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers serving a number of Google products, including Google Analytics. Learn more about our ISO compliance, and download our certificate (PDF) or learn more about ISO 27001.

Information security

In web-based computing, security of both data and applications is critical. Google dedicates significant resources towards securing applications and data handling to prevent unauthorized access to data.

Data is stored in an encoded format optimized for performance, rather than stored in a traditional file system or database manner. Data is dispersed across a number of physical and logical volumes for redundancy and expedient access, thereby obfuscating it from tampering.

Google applications run in a multi-tenant, distributed environment. Rather than segregating each customer's data onto a single machine or set of machines, data from all Google users (consumers, business, and even Google's own data) is distributed among a shared infrastructure composed of Google's many homogeneous machines and located in Google's data centers.

In addition, Google Analytics ensures secure transmission of its JavaScript libraries and measurement data. Google Analytics by default uses HTTP Strict Transport Security (HSTS), which instructs browsers that support HTTP over SSL (HTTPS) to use encryption protocol for all communication between end users, websites, and Google Analytics servers. Learn more

Operational security and disaster recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implements a comprehensive disaster-recovery program at all of its data centers. This program includes multiple components to eliminate single points of failure, including the following:

Data replication To help ensure availability in the event of a disaster, Google Analytics data stored in Google's distributed file system is replicated to separate systems in different data centers.

Geographical distribution of data centers Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region.

Resilient and redundant infrastructure Google's computing clusters are designed with resiliency and redundancy in mind, helping minimize single points of failure and the impact of common equipment failures and environmental risks.

Continuity plan in the event of disaster In addition to the redundancy of data and regionally dispersed data centers, Google also has a business-continuity plan for its headquarters in Mountain View, CA. This plan accounts for major disasters, such as a seismic event or a public-health crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers.

Give feedback about this article

Was this helpful? Yes No

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

Privacy controls in Google Analytics

Site and/or app owners using Google Analytics and Google Analytics for Firebase (aka "customers") may find this a useful resource, particularly if they are businesses affected by the European Economic Area's General Data Protection Regulation (GDPR), or other similar regulations.

For additional information, refer to Safeguarding your data.

In this article

Disable Analytics data collection (app)
Disable Analytics data collection (web)
Disable collection of granular location and device data
Redact email addresses and user-defined URL query parameters
Disable collection of Google signals data
Disable advertising features (app)
Disable advertising features (web)
Disable advertising personalization (app)
Disable advertising personalization (web)
IP Masking
Set the retention period for the Analytics data you collect
User-level Data Access and Portability
Delete end user data stored on a mobile device
Delete end user data stored on Analytics servers
Allow for / Disable Ads Personalization for any property
Use the Google Analytics for Firebase iOS SDK to verify app installation

Disable Analytics data collection (app)

You can programmatically disable data collection from Android and iOS apps that use the

- Google Analytics for Firebase SDK (instructions)
- Google Analytics Android SDK (instructions)
- Google Analytics iOS SDK (instructions)

Learn more about the data that Google Analytics and Google Analytics for Firebase collect.

Disable Analytics data collection (web)

You can programmatically disable data collection from

- Google Analytics 4 properties with gtag.js (instructions)
- Universal Analytics properties with gtag.js (instructions)
- Universal Analytics properties with analytics.js (instructions)
- Universal Analytics properties with ga.js (instructions)

Users of your website can also opt out from data collection using the Google Analytics opt-out browser add-on.

Disable collection of granular location and device data

You have the option to enable/disable the collection of granular location-and-device data on a per-region basis. Analytics collects this data by default. If you disable this data collection, Analytics does not collect the following data:

- City
- Latitude (of city)
- Longitude (of city)
- Browser minor version
- Browser User-Agent string
- Device brand
- Device model
- Device name
- Operating system minor version
- Platform minor version
- Screen resolution

If you edit the settings and disable collection for a region, then Analytics maintains any historical data that you've collected but no additional data is collected from the time of the change forward.

Learn more

> If you disable the collection of granular location and device data for a region, then modeled key events (i) volume is significantly reduced for that region. Downstream key event modeling and reporting in linked Google Ads and Search Ads 360 accounts is also impacted.

Redact email addresses and user-defined URL query parameters

You can configure your web data streams to perform client-side text redaction of email addresses and user-defined URL query parameters.

Learn more about Data redaction.

Disable collection of Google signals data

When you activate Google signals, you have the option to enable or disable collection of those signals on a per-region basis. If you edit Google-signals settings and disable collection for a region, then Analytics maintains any historical data that you've collected but no additional data is collected from the time of the change forward. If you disable collection of Google-signals data, you will not have access to remarketing lists based on Analytics data, advertising reporting features, or demographics and interests.

Learn more

> If you deactivate Google signals, then remarketing is not available for the impacted regions. Downstream key event modeling and reporting in linked Google Ads accounts is also impacted.

Disable advertising features (app)

You can programmatically disable collection of data for advertising features from Android and iOS apps that use the:

- Google Analytics for Firebase SDK (instructions)
- Google Analytics Android SDK (instructions)
- Google Analytics iOS SDK (instructions)

Learn more about the data that Google Analytics and Google Analytics for Firebase collect.

Disable advertising features (web)

You can programmatically disable collection of data for advertising features from:

- Google Analytics 4 properties with gtag.js (instructions)
- Universal Analytics properties with gtag.js (instructions)
- Universal Analytics properties with analytics.js (instructions)

Disable advertising personalization (app)

You can programmatically disable advertising personalization for data from Android and iOS apps that use the Google Analytics for Firebase SDK (instructions).

Learn more about the data that Google Analytics and Google Analytics for Firebase collect.

Disable advertising personalization (web)

You can programmatically disable advertising personalization for data from:

- Google Analytics 4 properties with gtag.js (instructions)
- Universal Analytics properties with gtag.js (instructions)
- Universal Analytics properties with analytics.js (instructions)

IP Masking

IP masking is available in Google Analytics for both web and app. Learn how IP masking works.

Universal Analytics properties

You can mask IP addresses for Universal Analytics properties using

- gtag.js (instructions)
- analytics.js (instructions)
- ga.js (instructions)

Google Analytics 4 properties

In Google Analytics 4, IP masking is not necessary since IP addresses are not logged or stored.

Set the retention period for the Analytics data that you collect

You can set the retention period for data you collect from

- Universal Analytics properties (instructions)
- Google Analytics 4 properties (for websites) (instructions)
- Google Analytics for Firebase. You can choose to retain user data for a maximum of 14 months or retain data according to the Analytics default data-retention policy (instructions)

User-level Data Access and Portability

For Universal Analytics properties, you can pull event information for any given user identifier via the User Explorer report or the User Activity API. These features allow you to analyze and export event level data for a single user identifier. In addition, 360 customers can integrate with BigQuery to create a full export of all event data associated with their users in a single queryable repository.

For Google Analytics 4 properties, the same functionality exists within Explorations. You can pull event information for any given user identifier via the User Explorer report or the User Activity report. These features allow you to analyze and export event level data for a single user identifier. You can also use the User Activity report to delete individual user records. In addition, you can integrate with BigQuery to create a full export of all event data associated with users in a single queryable repository.

Delete end user data stored on a mobile device

The Google Analytics for Firebase SDK lets you add controls to your app so that users can delete Analytics data stored locally on their mobile devices, and reset the app-instance ID in the process. Learn more about using `resetAnalyticsData` on Android and iOS.

The SDK also lets you control whether or not any Analytics data is collected from the app on a specific device. Learn more about using `setAnalyticsCollectionEnabled` on Android and iOS.

Delete end user data stored on Analytics servers

You can use the Google Analytics API to honor requests from users to delete data about them from Analytics servers on a per-app, per-device basis. Learn more about the User Deletion API.

Allow for / Disable ads personalization for any property

You can control whether data collected from end users for any property may be used for ads personalization via the advanced setting to allow for ads personalization.

Use the Google Analytics for Firebase iOS SDK to register attribution with SKAdNetwork

Unless app developers choose to opt out via a static configuration flag (instructions), the Google Analytics for Firebase (GA4F) iOS SDK will automatically call, upon first open, Apple's SKAdNetwork registerAppForAdNetworkAttribution API, which provides app-install-validation information to ad networks registered with Apple.

The SKAdNetwork API has been updated for iOS 14 and will be relied on more heavily for app-install attribution due to Apple's new privacy and security features announced in WWDC 2020, which now require app developers to obtain consent via a privacy-disclosure pop-up before using the Identifier for advertisers (IDFA) to track iOS users.

Give feedback about this article

Was this helpful? Yes No

Data privacy and security
Safeguarding your data
Privacy controls in Google Analytics
[GA4] Data redaction
Introduction to user consent management
[GA4] Verify and update consent settings in Google Analytics
[GA4] Behavioral modeling for consent mode
Google Analytics opt-out browser add-on
[UA] IP masking in Universal Analytics
[GA4] Policy requirements for Google Analytics Advertising Features
[UA] Security and privacy in Universal Analytics
Data Processing Terms
We use our own products
Data retention
[GA4] Data-deletion requests
Data deletion requests (Universal Analytics)
ISO 27001 Certification
Google Analytics links overview
Account setup with additional privacy features
Best practices to avoid sending Personally Identifiable Information (PII)
Policy Against Fingerprints and Locally Shared Objects
Data controls in Universal Analytics
Data controls in Google Analytics 4
[GA4] EU-focused data and privacy
HIPAA and Google Analytics
Data sharing settings

Choose your own learning path
Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.
Start learning today!

©2024 Google - Privacy Policy - Terms of Service

HIPAA and Google Analytics

Google Analytics is a measurement solution that can be used to obtain business insights about traffic on your websites and apps. It is important to ensure that your implementation of Google Analytics and the data collected about visitors to your properties satisfies all applicable legal requirements.

Please remember that to protect user privacy, Google Analytics policies and terms mandate that no data be passed to Google that Google could recognize as personally identifiable information (PII), and no data you collect using Google Analytics may reveal any sensitive information about a user, or identify them. If you need to delete data from the Analytics servers for any reason, you can schedule a data-deletion request or use the User Deletion API.

What is HIPAA and to whom does it apply?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that applies to HIPAA-regulated entities. The law and its implementing regulations typically are not relevant to Google Analytics customers operating exclusively outside of the US, nor are they relevant to every customer operating within the US. Analytics customers are responsible for determining whether they are HIPAA-regulated entities and what their obligations are under HIPAA.

Can Google Analytics be used in compliance with HIPAA?

Customers must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies. Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.

For HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the HHS bulletin provides specific guidance on when data may and may not qualify as PHI. Here are some additional steps you should take to ensure your use of Google Analytics is permissible:

- Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered.
- Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages.
- Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages..
- Please work with your legal team to identify pages on your site that do not relate to the provision of health care services, so that your configuration of Google Analytics does not result in the collection of PHI.

Give feedback about this article

Was this helpful? Yes No

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

©2024 Google - Privacy Policy - Terms of Service

English

Data sharing settings

There are several data sharing settings in your Analytics account. These settings let you customize how you share with Google the data that you collect using an Analytics data collection method (like the JavaScript tracking code, mobile SDKs, and the Measurement Protocol), so you can be more open or more restrictive with your data based on your own preferences. These settings only let you customize how you share the data you collect from websites, mobile apps, and other digital devices using Analytics. They do not apply to data about your Analytics account or how your account is used, like the number of properties and which additional features are set up. Regardless of your data sharing settings, your Analytics data may also be used only insofar as necessary to **maintain and protect** the Analytics service.

All Google representatives that can access account data, including vendors, must agree to internal access policy terms and conditions. Data access requires appropriate authentication; all access is over SSL and is logged for security review, and representatives can only use Google-approved computers when accessing customer data.

In this article:

Change your data sharing settings
Details and benefits of each data sharing setting
Controller-Controller Data Protection terms
Related resources

Change your data sharing settings

You need the Editor role to use this feature.

You must customize your data sharing settings when you sign up for an Analytics account, but you can return to the Admin section of an account and change the settings any time.

To change the data sharing settings:

1. In **Admin**, under *Account*, click **Account details**.
2. Edit any setting and click **Save**.

Details and benefits of each data sharing setting

Review the settings in your account, and this additional information here, to help you decide whether to turn these settings ON or OFF. If all settings are OFF, your Analytics data is only used to provide and maintain the Analytics service.

Google products & services

When you turn this setting ON, Google can access and analyze data to better understand online behavior and trends, and use this data to improve Google products and services. For example, this data can be used to improve the Google Ads system tools that you use to create, manage, and analyze your ad campaigns.

Any data collected and used by Google under the "Google products & services" setting is subject to the Controller-Controller Data Protection terms and Google is, for GDPR purposes, an independent controller of such data.

> **Note**: This data sharing option is not available to Analytics accounts with properties in the "Health" and "Finance" property industry categories. You can see your property industry category by going to **Admin** > **Property** > **Property details**.

Modeling contributions & business insights

Aggregated data can be used to help create features and publications that give you a better understanding of what's happening across your entire industry. When you share data for modeling contributions and business insights, that data is aggregated with data from other websites and apps, so it cannot be used to identify your organization, account, or users.

When you turn this setting OFF, data can still flow between Analytics and the other Google products that are explicitly linked to any of your account properties.

You benefit when this setting is ON because Analytics data can be used to help build better tools and provide guidance that can help your marketing and analysis efforts. Benchmarking data lets you know where you stand in your industry and contributes to research analyses that uncover important market trends, like year-over-year increase in mobile traffic.

Technical support

Analytics support representatives sometimes need to access your account to provide service and resolution to technical issues. When you turn this setting ON, support representatives can access your data to help resolve technical issues. If you turn this setting OFF, support representatives might not be able to help resolve technical issues.

You benefit when this setting is ON because Google support could access your account to troubleshoot and help you find solutions if you report an issue in your account.

Recommendations for your business

When you turn this setting ON, Google can access your Google Analytics account data, including account usage and configuration data, product spending, and users associated with your Google Analytics account.

You benefit when this setting is ON because Google can use your account data to help you make the most of Google products, providing you with insights, offers, recommendations, and optimization tips across Google Analytics and other Google products for business.

Controller-Controller Data Protection terms

When Google Analytics customers enable the data sharing setting for "Google products & services", Google is, for GDPR purposes, a controller of the data that is shared and used under this setting.

Learn more about Controller-Controller Data Protection terms

Related resources

- See what other Google products your Analytics account is linked to
- The Analytics security and privacy principles

Give feedback about this article

Was this helpful? Yes No

Data privacy and security
Safeguarding your data
Privacy controls in Google Analytics
[GA4] Data redaction
Introduction to user consent management
[GA4] Verify and update consent settings in Google Analytics
[GA4] Behavioral modeling for consent mode
Google Analytics opt-out browser add-on
[UA] IP masking in Universal Analytics
[GA4] Policy requirements for Google Analytics Advertising Features
[UA] Security and privacy in Universal Analytics
Data Processing Terms
We use our own products
Data retention
[GA4] Data-deletion requests
Data deletion requests (Universal Analytics)
ISO 27001 Certification
Google Analytics links overview
Account setup with additional privacy features
Best practices to avoid sending Personally Identifiable Information (PII)
Policy Against Fingerprints and Locally Shared Objects
Data controls in Universal Analytics
Data controls in Google Analytics 4
[GA4] EU-focused data and privacy
HIPAA and Google Analytics
Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?
Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

About enhanced conversions

Note: The global site tag (gtag.js) is now the Google tag. With this change, new and existing gtag.js installations will get new capabilities to help you do more, improve data quality, and adopt new features – all without additional code. Learn more About the Google tag.

Enhanced conversions is a feature that can improve the accuracy of your conversion measurement and unlock more powerful bidding. It supplements your existing conversion tags by sending hashed first party conversion data from your website to Google in a privacy safe way. The feature uses a secure one-way **hashing algorithm** called **SHA256** on your first party customer data, such as email addresses, before sending to Google. You can learn more about Google's conversion modeling solutions.

Note: Google is committed to protecting the confidentiality and security of your data. We'll keep your data confidential and secure using the same industry-leading standards we use to protect our own users' data. We only report aggregated and anonymized conversions. You can read more about enhanced conversions customer data policies and how we use your data.

How it works

When a customer completes a conversion on your website, you may receive first-party customer data such as an email address, name, home address, and/or phone number. This data can be captured in your conversion tracking tags, hashed, sent to Google in its hashed form, and then used to enhance your conversion measurement.

Depending on which type of enhanced conversions you use, the hashed data will be used in different ways to improve your measurement:

Enhanced conversions for web	Enhanced conversions for leads
Relevant for **advertisers who want to track sales and events that happen on a website.**	Relevant for **advertisers who want to track sales that happen off a website (for example, phone or email) from website leads.**
Improves measurement of **online conversions.**	Improves measurement of **offline transactions that came from a website lead or visitor.**
Allows you to send hashed first-party, user-provided data from your website when a user converts. The data is then used to match your customers to Google accounts, which were signed-in to when they engaged with one of your ads.	Allows you to use hashed, first-party user-provided data from your website lead forms for offline lead measurement. When you upload your leads, the provided hashed information is used to attribute back to the Google Ad campaign.

Enhanced conversions for web

With enhanced conversions for web, first-party customer data such as an email address, name, home address, or phone number is captured in your conversion tracking tags, hashed, sent to Google in its hashed form, and then used to match your customers to Google accounts, which were signed-in to when they engaged with one of your ads.

Benefits:

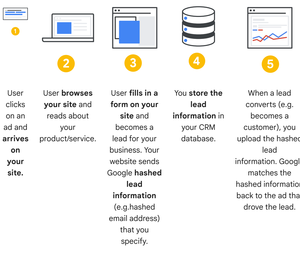
- Recover conversions that otherwise wouldn't have been measured
- Improve bidding optimization through better data
- Privacy safe with hashing of first-party customer data

Set up enhanced conversions for web

You can set up enhanced conversions for web in three ways:

1. **Google Tag Manager:** If you currently use Google Tag Manager for conversion tracking you can set up enhanced conversions for web manually with Google Tag Manager with only slight changes to your configuration.
2. **The Google tag:** If you currently have conversion tracking implemented using the Google tag directly on your page (not within a third-party tool or iFrame), you can set up enhanced conversions for web with your Google tag by making slight changes to your configuration.
3. **Google Ads API:** If you would like to provide enhanced conversions data via API in order to have more flexibility and control over your data, you can set up enhanced conversions for web using Google Ads API.

Enhanced conversions for leads



You can upload or import conversion data into Google Ads using first-party customer data from your website lead forms. Unlike the standard version of offline conversion imports, enhanced conversions for leads doesn't require you to modify your lead forms or customer relations management (CRM) systems to receive a **Google Click ID (GCLID)**. Instead, it uses information that was already captured about your leads, like email addresses, to measure conversions.

Benefits:

- **Easy to set up:** Configure measurement entirely from your Google Ads account.
- **Better performance:** Optimize your campaigns to sales and transactions that happen off your website.
- **Flexible:** Implement using the Google tag or with Google Tag Manager.

If you want to use a GCLID to track conversions when they occur, the existing GCLID-based upload method is still available. Learn more about how to set up offline conversions using GCLID

Set up enhanced conversions for leads

You can set up enhanced conversions for leads in two ways:

1. **Google Tag Manager:** If you currently use Google Tag Manager for conversion tracking you can set up enhanced conversions for leads with Google Tag Manager with only slight changes to your configuration.
2. **The Google tag:** If you currently have conversion tracking implemented using the Google tag directly on your page (not within a third-party tool or iFrame), you can set up enhanced conversions for leads with your Google tag by making slight changes to your configuration.

See what other users are saying about enhanced conversions

Join the conversation in the Ads Community

Related links

- About enhanced conversions for web in the Google Ads API
- Set up enhanced conversions for web manually with Google Tag Manager
- Set up enhanced conversions for web manually with the Google tag
- Set up enhanced conversion for leads with the Google tag
- Customer data policies
- Your guide to conversion modeling

Give feedback about this article

Was this helpful? Yes No

Enhanced conversions for web
About enhanced conversions
Enhanced conversions for web impact results
About the enhanced conversions for web Ads API diagnostics report
Set up enhanced conversions for web using the Google tag
Set up enhanced conversions for web using Google Tag Manager
About enhanced conversions for web in the Google Ads API

Achieve your advertising goals today!
Attend our Performance Max Masterclass, a livestream workshop session bringing together industry and Google ads PMax experts.
Register now

©2024 Google - Privacy Policy - Terms of Service - Google Ads Advertising Policies - About the Help Center
English

[GA4] EU-focused data and privacy

When collecting data, Google Analytics 4 does not log or store IP addresses.

- Analytics drops any IP addresses that it collects from EU users before logging that data via EU domains and servers.

In addition, Analytics provides controls to:

- Disable collection of Google-signals data on a per-region basis
- Disable the collection of granular location and device data on a per-region basis

Analytics does not log IP addresses

Google Analytics 4 does not log or store individual IP addresses.

Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases.

When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing.

EU data is collected in the EU

Google Analytics 4 collects all data from EU-based devices (based on IP-geo lookup) through domains and on servers based in the EU before forwarding traffic to Analytics servers for processing.

If you currently use a Content Security Policy (CSP), update your configurations (img-src and connection-src directives) to allow the following domains used by Analytics:

- *.google-analytics.com
- *.analytics.google.com

Regional controls

Google signals

When you activate Google signals, you have the option to enable or disable collection of those signals on a per-region basis. If you edit Google-signals settings and disable collection for a region, then Analytics maintains any historical data that you've collected but no additional data is collected from the time of the change forward. If you disable collection of Google-signals data, you will not have access to remarketing lists based on Analytics data, advertising reporting features, or demographics and interests. Learn how to Activate Google signals for Google Analytics 4 properties.

> If you deactivate Google signals, then remarketing is not available for the impacted regions. Downstream conversion modeling and reporting in linked Google Ads accounts is also impacted.

Collection of granular location and device data

You have the option to enable/disable the collection of granular location-and-device data on a per-region basis. Analytics collects this data by default. If you disable this data collection, Analytics does not collect the following data:

- City
- Latitude (of city)
- Longitude (of city)
- Browser minor version
- Browser User-Agent string
- Device brand
- Device model
- Device name
- Operating system minor version
- Platform minor version
- Screen resolution

If you edit the settings and disable collection for a region, then Analytics maintains any historical data that you've collected but no additional data is collected from the time of the change forward.

Learn more about Collecting granular location and device data.

> If you disable the collection of granular location and device data for a region, then modeled-conversion volume is significantly reduced for that region. Downstream conversion modeling and reporting in linked Google Ads and Search Ads 360 accounts is also impacted.

Give feedback about this article

Was this helpful? Yes No

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

©2024 Google - Privacy Policy - Terms of Service

English

[UA] Enable Remarketing and Advertising Reporting Features in Analytics

If you activate Google signals, the controls to enable Remarketing and Advertising Reporting Features are replaced by the Google-signals control.

This article explains how to configure Analytics so you can create remarketing audiences and share them with your advertising accounts. For example, you can create an audience of users who left items in their shopping carts but didn't complete their purchases, and then share that audience with Google Ads so you can reengage those users with follow-up ads.

Learn more about remarketing audiences in Analytics

In this article:

Prerequisites
Limits
Enable Remarketing and Advertising Reporting Features for a web property
Enable Remarketing and Advertising Reporting Features for an app
Related resources

Prerequisites

To take advantage of Remarketing with Analytics and Remarketing Lists for Search Ads with Analytics:

- Enable *Remarketing* and *Advertising Reporting Features*.

  When you enable those features, you also see data in the Demographics and Interests reports, see GDN Impression data in the Multi-Channel Funnel reports, and can take advantage of Google Marketing Platform integrations.

  To enable Remarketing and enable Advertising Reporting Features for a web property, you need to have the Editor role for that property. The Editor role is also required to create and edit audiences.
- Adhere to the Policy requirements for Analytics Advertising Features.
- Agree to the Analytics Terms of Service (please review them as they may have changed since you last viewed them)
- Have at least one active Google Ads or Display & Video 360 account that is linked to your Analytics property
- If you're using your audiences in Google Ads, add them to an ad group.

Limits

Keep in mind that there is limit of 2000 Remarketing Audiences per Analytics account.

The *In-Market Segments* dimension is not available for Remarketing Audiences.

The *Days Since Last Visit* metric is not available for Remarketing Audiences.

Enable Remarketing and Advertising Reporting Features for a web property

When you enable Remarketing for a web property, you can create remarketing audiences from your Analytics data, and share those audiences with your linked advertising accounts (e.g., Google Ads and Display & Video 360) and with Optimize.

When you enable Advertising Reporting Features for a web property, Analytics collects the information it normally does, as well as Google advertising cookies when those cookies are present.

You can enable Remarketing and Advertising Reporting Features for a web property by using one of the following methods:

- Modifying your property settings
- Modifying your tracking code
- Selecting the option to use existing tracking code when you're creating a Google Ads remarketing campaign

Modify your property settings

This method applies only to web properties, and to pages on which you're using gtag.js, analytics.js, or AMP tagging.

Modifying your property settings is also the only method by which you can use the Analytics tag to create remarketing lists for search ads.

When you modify your property settings to support Remarketing and/or Data Collection for Advertising Features, then traffic to all your pages is subject to this type of data collection. If you want to implement these features for only portions of your site, then you need to modify the tracking code for each relevant page, and leave these property settings off.

To update your property settings:

1. Sign in to your Analytics account.
2. Click **Admin**, and navigate to the **property** for which you want to enable these features.
3. In the *Property* column, click **Tracking Info**, then click **Data Collection**.
4. Under *Data Collection for Advertising Features*:
   - To enable Remarketing, set *Remarketing* and *Advertising Reporting Features* to **ON**.
   - To enable only the Advertising Reporting Features, set only *Advertising Reporting Features* to **ON**.

If you have previously enabled Remarketing and the Advertising Reporting Features by updating your tracking code, you can still implement these property settings and not incur any conflicts. This applies to Remarketing only on the Google Display Network.

Keep in mind that this method is only effective for enabling these features as they relate to your website users. If you want to enable these features as they relate to your app users, then you need to update your app-tracking code per the methods outlined for Android and iOS.

If you do *not* want to collect data for Advertising Features, then make sure that both of these options are set to **OFF**, and that your tracking code is not configured to collect this data.

You also have the option to activate Google signals to enhance Remarketing and reporting. If you activate Google signals, then those controls replace the ones for Remarketing and Advertising Reporting Features.

Alternative: Modify your tracking code

The preferred method of enabling Remarketing and Advertising Reporting Features is to modify your property settings as described above, though you can enable these features by modifying your tracking code.

If you want to enable Remarketing Lists for Search Ads, you need to use the property settings described above.

If you choose to enable Display Remarketing and the Advertising Reporting Features by updating your tracking code, you need to make only a simple, one-line change to your code as described in the following sections. This modification does not impact any customizations you have previously made to your code.

If you want to manually disable Advertising Reporting Features, you can modify your tracking code as described in the relevant sections below.

To enable these features for Universal Analytics, insert the bold line into your existing tracking code between the `'create'` and `'send'` commands, as in this example:

```
<script>
(function(i,s,o,g,r,a,m)
{i\'GoogleAnalyticsObject\']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[])).push(arguments)},i[r].l=1*new
Date();a=s.createElement(o),
m=s.getElementsByTagName(o)
[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','//www.google-
analytics.com/analytics.js','ga');
ga('create', 'UA-XXXXXX-XX', 'example.com');
ga('require', 'displayfeatures');
ga('send', 'pageview');
</script>
```

To revert the change, simply remove the line `ga('require', 'displayfeatures');`

To override the `displayfeatures` plugin and the property settings to turn off Advertising Reporting Features, add
`ga('set', 'allowAdFeatures', false); //to re-enable, set allowAdFeatures to true`
after the `create` command, and before the hit is sent.

If you're using Google Tag Manager, follow these instructions to edit the Analytics tag.

If you're still using the ga.js tracking code, you can find instructions for modifying that code here.

Alternative: Select the option to use existing tracking code when you're creating Google Ads remarketing campaign

When you're creating a remarketing campaign in Google Ads, if you're account is linked to an Analytics account, then you have an option to *use the tracking code that's already on your website* rather than have Google Ads generate a remarketing tag for you. If you use this option, then Remarketing is automatically enabled in Analytics. Learn more about creating remarketing campaigns in Google Ads.

Enable/disable Remarketing and Advertising Reporting Features for an app

When you enable these features for an app, then Analytics collects the information it normally does, as well as information associated with mobile-advertising IDs.

To enable/disable these features for an app, you need to modify the Analytics tracking code that you have included in your app code. The examples below explain how to modify the tracking code for Android and iOS apps.

App-tracking code change for Android

To enable these features for Android, modify your Analytics tracking code to collect the advertising id. Call the `enableAdvertisingIdCollection` method on the tracker for which you want to enable these features. For example:

```
// Get tracker.
Tracker t = ((AnalyticsSampleApp)
getActivity().getApplication()).getTracker(
TrackerName.APP_TRACKER);

// Enable Display Features.
t.enableAdvertisingIdCollection(true); // to disable Display
Features, set this value to false
```

Learn more about supporting Display Advertising on Android

App-tracking code change for iOS

To enable these features for iOS, collect the IDFA (Advertising Identifier). To enable IDFA collection, link the `libAdIdAccess.a` and `AdSupport.framework` libraries to your application and set the `allowIDFACollection` to **YES** on each tracker that will collect the IDFA. For example:

```
// Assumes a tracker has already been initialized with a property
ID, otherwise
// getDefaultTracker returns nil.
id tracker = [[GAI sharedInstance] defaultTracker];

// Enable IDFA collection.
tracker.allowIDFACollection = YES; // to disable Display Features,
set this value to NO
```

If you're using Google Tag Manager, follow these instructions to edit the Analytics tag.

Related resources

- Policy requirements for Analytics Advertising Features
- Google Privacy & Terms

Give feedback about this article

Was this helpful? Yes No

Remarketing with Analytics
[UA] About remarketing audiences in Analytics
[UA] Enable Remarketing and Advertising Reporting Features in Analytics
[UA] Dynamically disable Advertising Features or Advertising Personalization in Google Analytics
[UA] Create and edit audiences
[UA] Use your remarketing audiences in Google Ads
[UA] State-based audiences
[UA] Smart Lists
[UA] Remarketing audiences you create
[UA] Remarketing Lists for Search Ads with Analytics
[UA] How Analytics sampling and processing can affect remarketing audiences
[UA] Test remarketing campaigns
[UA] Troubleshoot Analytics Remarketing issues

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?
Sign in for additional support options to quickly solve your issue
Sign In

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

The Google Analytics: GA4 Configuration tag is now the Google tag. GA4 Configuration tags in a web container will be automatically migrated starting in September. There are no changes to your existing measurement and there is no action required from you. Learn more

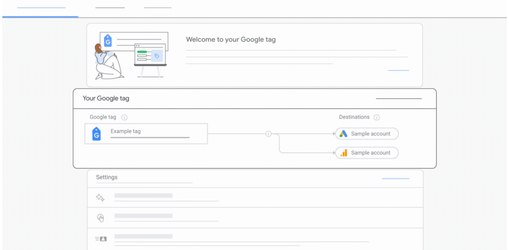
Before you begin
About the Google tag
Introduction to user consent management
About consent mode
Destination ID: Definition
Google tag ID: Definition
Destination: Definition

About the Google tag

Note: The global site tag (gtag.js) is now the Google tag. With this change, new and existing gtag.js installations will get new capabilities to help you do more, improve data quality, and adopt new features – all without additional code.

The Google tag (gtag.js) is a single tag you can add to your website to use a variety of Google products and services. Instead of managing multiple tags for different Google product accounts, you can use the Google tag across your entire website and connect the tag to multiple destinations.

The Google tag lets you send data from your website to linked Google product **destinations** to help you measure the effectiveness of your website and ads. The Google tag is currently only accessible and configurable from Google Ads, Google Analytics 4, and Campaign Manager 360.



As website technologies such as cookies continue to evolve due to privacy, browser, and regulation changes, having high-quality, site-wide tagging across your website is important to help ensure you're getting the most accurate measurement.

When you're ready, you can set up your Google tag.

How it works

Previously, you had to set up a global site tag (gtag.js). The global site tag has evolved into the Google tag.

Your Google tag (gtag.js) has a single **tag ID** you can add to your website to use a variety of Google products and services. Instead of managing multiple tags for different Google product accounts, you can use a single Google tag across your entire website and connect the tag ID to multiple **destinations**.

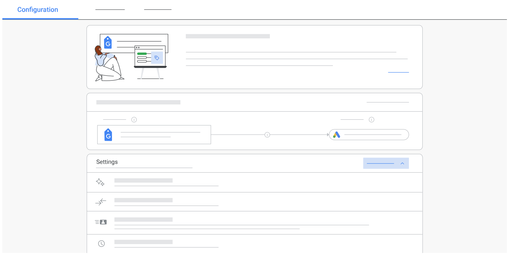
A new "Google tag" screen will replace the existing global site tag screens in Google Ads, Google Analytics, and Campaign Manager 360 letting you access measurement features without adding code after the initial set-up. Changing settings in your Google tag will affect all associated destinations.

Benefits

- **Multiple tags:** If you have more than one tag installed on your website, you can choose to combine your Google tags to help you get better data and manage them in one place.
- **Manage access:** You can also now manage user access to your tag settings separately from access to your other products, giving you more control over who has access to change your critical measurement settings.

What's changing

You'll now see a new Google tag screen in your Google Ads, Google Analytics, and Campaign Manager 360 accounts.



Note: All global site tags have been converted into Google tags. If you have a global site tag on your website, you don't need to update your site to use the Google tag.

When you're ready, you can:

1. Set up your Google tag
2. Set up and manage user consent
3. Configure your Google tag settings
4. Manage your Google tag (optional)
5. Manage Google tag users (optional)

User management

You can manage users in the "Admin" tab of your Google tag. The user management settings of the Google tag let you manage user access to your tag settings separately from access to your other products.

Security and privacy for website tracking

Google's security standards are strict. Google products only collect data on pages where you have deployed the associated tags.

Please ensure you're providing users with clear and comprehensive information about the data you collect on your websites, and getting consent for that collection where legally required.

Note: If you have not obtained users' consent for the collection, sharing, and use of personal data for personalization of ads where legally required, be sure to disable the collection of remarketing data. Learn how to modify the Google tag to disable the collection of remarketing data for specific users.

Related links

- Set up your Google tag
- Configure your Google tag settings
- Manage your Google tag
- Manage Google tag users

Give feedback about this article

Was this helpful? Yes No

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

©2024 Google - Privacy Policy - Terms of Service

English

[GA4] Measure activity across platforms with User-ID
[GA4] Best practices for User-ID
[GA4] Using first-party data to power durable and accurate measurement
[GA4] Enhanced conversions in Google Analytics
[GA4] User-provided data collection
[GA4] Set up user-provided data collection (gtag.js)
[GA4] Set up user-provided data collection (Tag Manager)

[GA4] Measure activity across platforms with User-ID

Send user IDs generated by your business to your Analytics property

The User-ID feature lets you associate your own identifiers with individual users so you can connect their behavior across different sessions and on various devices and platforms. Analytics interprets each user ID as a separate user, which provides you with more accurate user counts and a more holistic story about a user's relationship with your business.

When you collect user IDs and you have linked Analytics to BigQuery, that information is exported to BigQuery regardless of the consent status of your users.

Before you begin

To send user IDs to Analytics, you need to create a unique ID for each user on your own and assign and consistently reassign the IDs to your users. This is typically done during login. For example, when a user signs in, you could use their email address to generate a unique ID that you can reference throughout your website or application. Each user ID must be fewer than 256 characters long.

Note: You're responsible for ensuring that your use of the user ID is in accordance with theGoogle Analytics Terms of Service. This includes avoiding the use of impermissible personally identifiable information, and providing appropriate notice of your use of identifiers in your Privacy Policy. Your user ID must not contain information that a third party could use to determine a user's identity.

Send user IDs

For instructions on how to send a user ID, check Send user IDs.

Verify the reporting identity

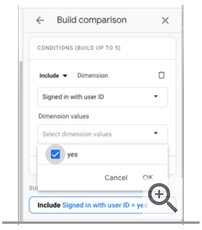
Make sure your property uses a reporting identity that includes the User-ID option by doing the following:

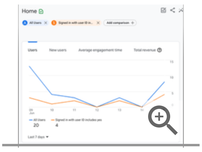
1. In **Admin**, under *Data display*, click **Reporting Identity**.
2. Select either:
   - **Blended**: evaluates user ID, device ID, modeled data
   - **Observed**: evaluates user ID, device ID

What you can do with User-ID

Compare signed in with non-signed in users

To compare the behavior of users who are signed in with the behavior of users who aren't signed in, build a comparison that uses the *Signed in with user ID* dimension and set the dimension value to "yes".





User exploration

The user exploration displays the users who make up an existing segment, or who make up the temporary segment that results from using other Explorations techniques. You can drill down into the list to see detailed information about individual users, including how and when that user was acquired, summary metrics for that user, and a timeline of their activities on your site or app.

Create remarketing audiences based on User-ID data

You can create remarketing audiences based on user IDs. If you've linked your Google Analytics and Ads accounts, these audiences are available in your shared library in Google Ads.

- If you are using User-ID, then Analytics only includes the user identifier and the device identifier for the last device associated with each logged-in user.
- If you're not using User-ID, Analytics includes all device and user identifiers in the audience information it exports to Ads.

How Analytics handles sessions with incomplete User-ID collection

Users sometimes trigger events on your site or app before signing in or after signing out. In the first instance, Analytics uses the session ID to associate that session with the user ID provided when the user signs in. In the second instance, once a user signs out, Analytics stops associating any subsequent events with that user ID.

For example, a user starts a session with no associated user ID and triggers Events 1 and 2. No user ID is associated with those events. The user then signs in and triggers Event 3. Events 1, 2, and 3 are now all associated with that user's ID. The user finally signs out and then triggers Event 4. No user ID is associated with Event 4. Events 1, 2, and 3 remain associated with that user.

Limits

- The User-ID feature is built for use with Google Analytics technologies. All implementations must comply with the Analytics SDK / User-ID Feature Policy .
- The user IDs you send to Google Analytics must be fewer than 256 characters long.
- Any data in your Analytics account collected and recorded prior to implementation won't be reprocessed and associated with a user ID.
- User-ID data collected in one property can't be shared or mixed with data in other properties.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

User-provided-data collection for User-ID Policy

Your use of the user-provided-data collection feature for User-ID ("the feature"), and any optional integrations are subject to the following additional terms, which will govern in the case of any conflict between such terms and the terms governing your use of Google Analytics or Google Analytics 360 (as applicable):

1. Your use of the feature is subject to the Measurement Protocol, SDK and User ID policy.
2. You may only send first-party data (i.e., information shared directly with you by your end users) to Google through the feature, including via supported APIs, data import and/or measurement protocol.
3. Notwithstanding any prohibition against passing data to Google that it can recognize as personally identifiable information ("PII"), you may pass PII for the sole purpose of using this feature provided all the below requirements are met:
   a. You must hash any data you send through the feature that allows Google to personally identify an individual (such as email, phone numbers, first name and last name, and street address) using the SHA256 algorithm, which is the industry standard for one-way hashing.
      - Note that country, state, city and zip code data fields themselves should not be hashed.
      - If you use the Google Tagging Javascript API and/or Google Tag Manager to send data through the feature, any PII data collected therein will be automatically hashed.
   b. You must obtain consent from your end users for the collection, passing and use of any PII you send to Google through the feature, including their consent to associate data across their unauthenticated and authenticated session activities on your sites and/or apps. You must also obtain consent from your end users for the use of such PII sent through the API and/or through the feature, for any additional measurement, targeting, audience personalization and/or reporting activities, including those optionally enabled within Analytics and through your linking integrations.
   c. You acknowledge that any use of the feature in conjunction with ads measurement and/or audience features is subject to the Google Analytics Advertising Features Policy.
   d. If you implement Consent Mode feature of Google Analytics and/or Google Ads, the consent you procure from your end users for your use of their PII for the feature and/or associated integrations operates independently and is not affected by end user choices over the Consent Mode ad_storage setting and/or analytics_storage, which apply only to the cookies that are set as part of the analytics service or ads service as defined here and here.

Give feedback about this article

Was this helpful? Yes No

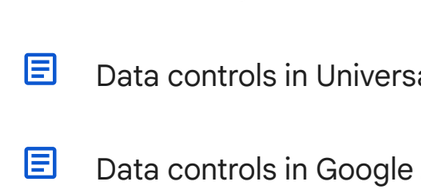
Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings



Choose your own learning path

Help guide

Help guide

Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.

Let's chat

©2024 Google - Privacy Policy - Terms of Service

English

[GA4] Policy requirements for Google Analytics Advertising Features

This article applies to both Google Analytics 4 and Universal Analytics.

Google Analytics Advertising Features let you enable features in Analytics that aren't available through standard implementations. Advertising features include:

- Remarketing with Google Analytics
- Google Display Network Impression Reporting
- Google Analytics Demographics and Interest Reporting
- Integrated services that require Google Analytics to collect data for advertising purposes, including the collection of data via advertising cookies and identifiers

By enabling the Advertising Features, you enable Google Analytics to collect data about your traffic via Google advertising cookies and identifiers, in addition to data collected through a standard Google Analytics implementation. Regardless of how you send data to Google Analytics (for example, via the Google Analytics tracking code, Google Analytics SDK, or the Measurement Protocol), if you use Google Analytics Advertising Features, you must adhere to this policy.

When you use Google Analytics Advertising Features, you are the sole controller under all applicable data protection legislation.

This means you will not identify users or facilitate the merging of personally identifiable information with additional information collected through any Google advertising product or feature unless you have robust notice of, and the user's prior affirmative (i.e., opt-in) consent to, that identification or merger, and are using a Google Analytics feature that expressly supports such identification or merger. Irrespective of users' consent, you must not attempt to disaggregate data that Google reports in aggregate.

Learn more about PII in Google's contracts and policies

If you've enabled any Google Analytics Advertising features, you are required to notify your visitors by disclosing the following information in your privacy policy:

- The Google Analytics Advertising Features you've implemented.
- How you and third-party vendors use first-party cookies (such as the Google Analytics cookie) or other first-party identifiers, and third-party cookies (such as Google advertising cookies) or other third-party identifiers together.
- How visitors can opt-out of the Google Analytics Advertising Features you use, including through Ads Settings, Ad Settings for mobile apps, or any other available means (for example, the NAI's consumer opt-out).

We also encourage you to point users to Google Analytics' currently available opt-outs for the web.

European Union user-consent policy

When using Google Analytics Advertising Features, you must also comply with the European Union User Consent Policy.

Japan user-consent policy

If you receive non-personally identifiable user information relating to Japanese users from Google in connection with your use of Google Analytics, you must not merge that information with personally-identifiable information unless, prior to such processing, you have obtained all legally required consents from the user and have provided Google with accurate and complete information about the processing via the Google Troubleshooter.

Interest-based advertising

If you've enabled interest-based advertising, including Remarketing, with Google Analytics in connection with other Google services, you must follow the policies applicable to those Google services (like the Google Ads Policy for Personalized advertising and its sensitive category restrictions, and the Platform Program Policies). If you use Google Analytics to collect sensitive information about your visitors, as described in the Google Ads sensitive category restrictions, you may not use Google Analytics to collect data for the purpose of interest based advertising. You can disable interest-based advertising via the advanced ads-personalization setting.

Because laws across countries and territories vary, and because Google Analytics can be used in many ways, Google is unable to provide the exact language you need to include in your privacy policy. Only you understand the unique aspects and special considerations of your business, and your privacy policy should account for this information that only you can provide.

This policy was last updated April 27, 2022.

Give feedback about this article

Was this helpful? Yes No

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- **[GA4] Policy requirements for Google Analytics Advertising Features**
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

Help guide

Help guide

Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.

Let's chat

Filter

Get started
Introduction to Google Analytics 4
Migrate from Universal Analytics

Set up measurement
Web measurement
The Google Tag and Tag Manager
Set up events
Add parameters
Send user IDs
Measure exceptions
Measure pageviews
Measure single page applications
Ecommerce measurement
App measurement

Measurement Protocol
Overview
Send events to Google Analytics
Send user-provided data
Validate events
Verify Implementation
User properties
Troubleshooting

Google Chrome is deprecating third-party cookies. Find out more: goo.gle/3pcd.

Send user IDs

On this page
Before you begin
Send user IDs

The User-ID feature lets you associate your own identifiers with individual users so you can connect their behavior across different sessions and on various devices and platforms.

This article describes how to send user IDs from your website once you've generated the user IDs. To learn more about the User-ID feature, see Measure activity across platforms. To learn how to set a user ID for an app, see Set a user ID instead.

Google tag | Tag Manager

Before you begin

This guide assumes that you've done the following:

- Create a Google Analytics 4 account and property
- Create a web data stream for your website
- Place the Google tag on your website

It also assumes that you have the following:

- Access to your website source code
- The Editor role to the Google Analytics account

Send user IDs

To send a user ID to Analytics, add the `user_id` parameter to the `config` command in the measurement code on each page of your website. Using the following snippet, replace `G-XXXXXXXX` with your tag ID and `USER_ID` with the generated user ID.

```
gtag('config', 'TAG_ID', {
  'user_id': 'USER_ID'
});
```

Was this helpful?

Except as otherwise noted, the content of this page is licensed under the Creative Commons Attribution 4.0 License, and code samples are licensed under the Apache 2.0 License. For details, see the Google Developers Site Policies. Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2024-04-10 UTC.

[GA4] First-party data
[GA4] Measure activity across platforms with User-ID
[GA4] Best practices for User-ID
[GA4] Using first-party data to power durable and accurate measurement
[GA4] Enhanced conversions in Google Analytics
[GA4] User-provided data collection
[GA4] Set up user-provided data collection (gtag.js)
[GA4] Set up user-provided data collection (Tag Manager)

[GA4] User-provided data collection

This feature is part of an open beta. Keep in mind that the feature is subject to change.

Overview

As a Google Analytics administrator or editor, you can set up user-provided data collection to send your consented, first-party data from your website to Google Analytics. The data you send is then matched with other Google data in a privacy-safe way to improve the accuracy of your measurement data and power enhanced Analytics capabilities.

If you are sending data from a website, you have the option to implement user-provided data collection using a secure one-way hashing algorithm called SHA256 to hash the data before sending it to Google, or you can rely on the feature to use the SHA256 hashing algorithm on the user-provided data before sending it to Google.

If you implement user-provided data collection through Measurement Protocol, you must use SHA256 to hash the data before sending it to Google.

This feature is not available for properties in the "Health" and "Finance" industry categories.

Benefits

User-provided data collection allows you to future-proof your setup so that it's not dependent on third-party cookies, which are going away. It also enables these features and functionality:

Enhanced conversions

User-provided data collection enables enhanced conversions support for Google Analytics 4 conversions. Enhanced conversions allows Google Analytics to produce a more complete picture of cross-device and conversion measurement and attribution using first-party data.

The integration matches your consented, hashed customer data with Google data to fill in gaps for Google Ads ad interactions that may be unobservable when cookies or other user identifiers are not available. It then uses this more holistic view to improve conversion modeling, bid optimization, and provide an improved view of cross-channel performance in GA4 and Google Ads reports.

Demographics and Interests

User-provided-data collection provides demographic and interest reporting based on first-party data and consented Google signed-in user data, helping to future-proof measurement without depending on third-party cookies.

Before you implement

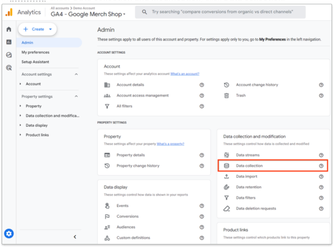
To send consented, first-party data from your website using user-provided data collection, you must link your Google Analytics property to your Google Ads account.

Acknowledging the user-provided data feature policy allows user-provided data collection on your property. Note that acknowledging the feature policy is **permanent** and will result in the following changes to your property. Though you can disable user-provided data collection from your tag, the following changes cannot be undone and should be reviewed before acknowledging the policy:

- This feature is intended for properties with web data streams. At this time, we do not recommend it if you have an app data stream. If you have an app data stream without a web data stream, use on-device measurement for iOS campaigns for similar reporting benefits in Analytics.
- To ensure the accuracy of your data, improvements to the models and attribution by enhanced conversions with Google Analytics are not available immediately. You should expect 1 month while it's active before these improvements are available in reports in Google Analytics and in the downstream reports and bidding in Google Ads.
- If your property has audiences with conditions that involve user interactions across multiple devices, audience membership will decrease since signed-in user data (User-ID) is kept separately from signed-out user data. This means that the ability to remarket to these audiences on devices other than the device where they met the audience condition criteria will be impacted. This impact will be partially mitigated if your property has enabled Google signals.
- Demographics and interest data for users with user ID will transition from being derived from cookie and device identifiers to user-provided data from signed-in users.

Instructions

1. Activate user-provided data collection.
   When you activate user-provided data collection, Google Analytics can collect user-provided data from all the data streams in the Google Analytics property and export that data to your linked advertising accounts.
   a. In **Admin**, under **Data collection and modification**, click **Data collection**.



   b. In **User-provided data collection**, click **Turn on**.
   c. (Optional) Select **Collect automatically detected user-provided data** to enable Google Analytics to detect user-provided data on your website automatically.

   Optional setting
   These settings can be updated after user-provided data is turned on.
   Collect automatically detected user-provided data.
   When turned on, Google Analytics will receive hashed, user-provided data that is automatically detected by the Google Tag on your website. Learn more about user-provided data collection
   Note: This feature requires that your Google Tag is configured to automatically detect user-provided data. User-provided data collection can be configured manually with the Google Tag or Google Tag Manager.

   If you select this option, you must also enable automatic collection in the Google tag. You can update this setting after you turn on user-provided data collection. If you enable the manual or code method, Analytics will automatically detect user-provided data only if the manual or code method doesn't identify user-provided data.
   d. Review the User-provided data policy, then click **Turn on**.
2. Identify and configure collection of user-provided data on your website through one of these options:

Implementation option	Details
gtag.js	If you currently use gtag.js to collect data from your website, you should follow the instructions for gtag.js to make slight adjustments to your configuration to collect user-provided data. Learn about the gtag.js implementation
Google Tag Manager	If you currently use Google Tag Manager to collect data from your website, you should follow the instructions for Tag Manager to update your container with variables that collect user-provided data. Learn about the Tag Manager implementation
Measurement Protocol	If you want to collect user-provided data from an offline interaction, you can set up user-provided data collection using Measurement Protocol. Learn about the Measurement Protocol implementation

Understanding when to implement the User-ID feature

User-provided data can be used with and without the user-ID feature. The User-ID feature uses your own unique user identifiers (which must be a different identifier from the ones used in user-provided data collection) that are created and managed by you for each user.

For some websites, implementing the User-ID feature may not be possible. But for other websites, such as ecommerce sites, we recommend that you set up the User-ID feature along with user-provided data collection to provide the most accurate user reporting in Analytics.

If you send user-provided data without also sending user IDs, collected user-provided data will be pseudonymized and used to recognize unique users for user deduplication and reporting purposes. When multiple types of user-provided data are provided, Analytics will prioritize in the following order: email, phone, name and address. Note that if user IDs are later provided for users that were previously measured with only user-provided data (no user ID), Analytics will recognize these as separate users for reporting purposes.

Sharing more than one field

You can include one or more fields from your site. By including more than one field, you increase the likelihood of a customer match and of attributing the conversion.

If you would only like to provide one field, we recommend sending email; however, the address and phone fields can also be helpful in improving the likelihood of matches.

Disabling user-provided data collection

While acknowledging the feature policy is permanent, you can stop collecting user-provided data in Analytics these ways:

- Toggling off **User-provided data collection** in your Google Analytics implementation via **Admin** > **Data Settings** > **Data collection** will turn off the ingestion and processing of user-provided data in your property.
- Toggling off **User-provided data collection** in your Tagging or Tag Manager implementation will stop the Google tag from sending user-provided data to your Analytics property. Additionally, if you send user-provided data to Analytics with Measurement Protocol, you'll want to update your implementation to stop including user-provided data.

Alternatively, if you are unable to modify the data being sent to Analytics, but you want to stop using the feature in reporting, you can disable Blended reporting in the Reporting Identity settings and therefore only use data from the anonymous identity space.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

[GA4] Reporting identity

Learn how Google Analytics measures users across devices and platforms.

An individual customer often interacts with your business using different devices and platforms. For example, someone might browse your products on a Pixel tablet at breakfast, do more research using a browser on their work computer at lunch, then make a purchase on their iPhone after dinner. While each of these activities is a separate session, Google Analytics 4 can use the following methods to unify them into a single cross-device user journey:

- User-ID
- User-provided data
- Device ID
- Modeling

Analytics creates a single user journey from all the data associated with the same identity. Because these identity spaces are used in all reports, they allow you to de-duplicate users and tell a more unified, holistic story about their relationships with your business.

Identity spaces

Collectively, the identifiers listed above are called *identity spaces*, and the identity space(s) used by your Analytics property is called its *reporting identity*.

User-ID

If you create your own persistent IDs for signed-in users, you can use these IDs to measure user journeys across devices. To use this identity space, you must consistently assign IDs to your users and include the IDs along with the data you send to Analytics. User-ID is the most accurate identity space, because it uses data you collect to identify your users.

Learn how to implement User-ID.

User-provided data

If you collect user-provided data (hashed, consented personal data) without user ID with the data you send to Google Analytics, user-provided data can serve as the identifier in the user-ID identity space. When this occurs, for each session, Analytics will prioritize the user-provided data in the following order: email, phone number, name and address.

Learn more about user-provided data collection.

Device-ID

Analytics can also use device ID as an identity space. On websites, the device ID gets its value from the client ID. On apps, the device ID is the app-instance ID.

Modeling

When users decline Analytics identifiers like cookies, behavioral data for those users is unavailable. Analytics fills this gap by using the data of similar users who do accept cookies from the same property to model the behavior of the users who decline cookies. Learn more

How Analytics determines the reporting identity

Analytics determines your reporting identity based on which identity spaces you choose to collect and which ones you make available via the following options.

Reporting identity options

- Blended: By User-ID, device ID, then modeling. Uses the user ID if it is collected. If User-ID information is not available, then Analytics uses the device ID. If no identifier is available, Analytics uses modeling.
- Observed: By User-ID, then device ID. Uses the user ID if it is collected. If User-ID information is not available, then Analytics uses the device ID.
- Device based: Uses only the device ID and ignores all other IDs that are collected.

To get the full benefit of the first two options, you need to collect user IDs. In addition, your property must have enough activity from signed-in users to adequately obfuscate their identity. As a consequence your reports are subject to data thresholds.

> **Note:** The option you choose does not affect data collection or processing. You can switch between the options at any time without making any permanent impact on data.

Set the reporting identity for your property

1. In **Admin**, under *Data display*, click **Reporting identity**.
2. Select the reporting identity you want to use.
3. Click **Save**.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

[GA4] About connected site tags

This article is for website owners who are setting up a Google Analytics 4 property and who are given the option (by the GA4 setup wizard) to reuse their existing Universal Analytics tagging.

If your Universal Analytics property uses **gtag.js** or **analytics.js** (including if analytics.js was deployed through a tag management system like Google Tag Manager), the GA4 Setup Assistant wizard can reuse your existing tagging (i.e., the tag being used by your Universal Analytics property). This tag reuse saves you from having to add the tag manually to your web pages and is made possible via a feature called connected site tags.

Be careful when deleting your Universal Analytics property or connected site tag
For website data to continue to flow to your GA4 property, you must keep your Universal Analytics property and connected site tag configuration.

The remainder of this article is for users with advanced implementation needs.

How it works

Here are a few points about how connected site tags work.

- An additional `gtag('config', 'G-XXXXXXXXXX')` call is made (without any parameters), which downloads a Google Analytics 4 tag container and sends an automatic page_view event to the Google Analytics 4 property.
- Enhanced measurement events (when enabled) are automatically collected in the Google Analytics 4 property, but are not collected in the Universal Analytics property.

  Note: If you use analytics.js to load your connected site tag, enhanced measurement events will be disabled in Google Analytics 4. You should consider replacing your analytics.js tag with gtag.js (the Google Tag).

- Any events sent via `gtag('event')` to the Universal Analytics property are also sent to the Google Analytics 4 property.
- Connected site tags require the full site to be consistently tagged using a gtag.js or analytics.js snippet (or deployed through a tag management system like Google Tag Manager) that is controlled by a single Universal Analytics property. If your Universal Analytics property receives data from mixed implementations (e.g., some pages are tagged with analytics.js or Google Tag Manager, while others with gtag.js), we recommend that you first retag your site with only gtag.js (the Google tag) or deploy a GA4 tag if using Google Tag Manager.

Considerations

The connected Google Analytics 4 tag is a way to send data to a Google Analytics 4 property without changing your deployed tags. For the best results, make sure that your site consistently tagged using a gtag.js or analytics.js snippet (or deployed through a tag management system like Google Tag Manager). Using different types of Google Analytics tags might lead to inconsistent data reports.

If you use analytics.js on your page, you won't be able to take advantage of all the features in Google Analytics 4. Here are a few examples of how using analytics.js can impact specific tagging controls for Google Analytics 4:

- Enhanced measurement events won't work
- Additional configuration of the Google Analytics 4 tag using the gtag.js API will be very limited, and you won't be able to add additional commands using the API

We encourage you to leverage the full set of Google Analytics 4 and deploy the Google tag on your page for the best Analytics experience.

Add / remove a connected site tag

If you configured a web site tag to send data to a Universal Analytics property, you can reuse this tag to send data to additional destinations like a GA4 property. You can do this in your **Universal Analytics property**:

Add a connected site tag

1. Sign in to your Google Analytics account, and make sure you're in your Universal Analytics property.
2. Click **Admin**.
3. In the *Property* column, click **Tracking Info**, then **Tracking Code.**
4. Click **Connected Site Tags**. (You might need to scroll down.)
5. On the *Connected Tags* page, enter the ID for the tag you want to add, then enter a name for the tag if you like.
6. Click **Connect**.

Enable a connected site tag through analytics.js

Navigate to the *Connected Tags* page following the instructions above, and add the Google tag ID. Check the box *Enable Connected tags through analytics.js* to reuse the analytics.js tag to send data to Google Analytics 4.

Remove a connected site tag

1. Sign in to your Google Analytics account, and make sure you're in your Universal Analytics property.
2. Click **Admin**.
3. In the *Property* column, click **Tracking Info**, then **Tracking Code.**
4. Click **Connected Site Tags**. (You might need to scroll down.)
5. On the *Connected Tags* page, go to the row for the tag you want to remove, and click ⋮ > **Remove tag**.

Add a GA4 tag to a page with connected site tags

If you're adding a GA4 tag and would still like to keep the existing connected site tags on your page, follow these rules to make sure events are sent correctly to GA4:

- If you're using analytics.js on the page, add the Google tag at the top of the page, to appear before the analytics.js tag.

  It's recommended that you have only one Google tag instance on your page at all times, with proper configuration.

- If you're deploying your Universal Analytics tag using Google Tag Manager, you can add your GA4 tags by following these steps.

Make sure to enable the "Ignore duplicate instances of on-page configuration" option as described below.

Ignore duplicate instances of on-page configuration

If the same tag is configured two or more times on the same page, it may result in duplicate data or mixed settings. Enable this option in your Google Analytics 4 property to ignore duplicate instances of on-page config commands.

1. In **Admin**, under *Data collection and modification*, click **Data streams**.
2. Click the specific data stream you'd like to configure.
3. In the *Google tag* section (at the bottom), click **Configure tag settings**.
4. In the *Google tag* screen, go to the *Admin* tab, and select **Manage Google tag**.
5. Enable **Ignore duplicate instances of on-page configuration**.
6. Click **Save**.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

©2024 Google - Privacy Policy - Terms of Service
English

[GA4] Advanced settings to allow for ads personalization

This article applies to both Google Analytics 4 and Universal Analytics.

Use the advanced settings to allow for ads personalization (in Property Settings) to enable or disable ads personalization for users coming from any/all supported countries and/or US States. The setting takes effect for data collection going forward and does not retroactively apply to data previously collected. Disabling ads personalization does not affect your ability to use analytics data from that property for measurement and content personalization (e.g., A/B testing in Firebase).

If you disable ads personalization for a given region, then all events collected from that location will be marked as not eligible for use for ads personalization - Non-Personalized Ads (NPA). This means that any **key events** from these regions will be marked as not for use for ads personalization even when exported to your linked ads accounts. In addition, any end user coming from a disabled location will not be added to any lists that may be exported to your linked ads accounts, although lists that have already been exported will not be affected.

All events collected for the property, and any audiences based on that data, are still available within Analytics for use in reports, explorations, and audience building, and can be exported to non-advertising products.

This setting remains effective even where you've configured the following:

- Analytics integrations that facilitate the import/export of audiences and key events with advertising and other products
- The inclusion / exclusion of events and user properties with regard to ads personalization
- The identification of any specific event as NPA, manually or aside from the effects of this control, during collection

To exclude property data from being used to personalize ads

You need the Editor role to manage these settings for a Google Analytics property.

In a Google Analytics 4 property

1. In **Admin**, under *Data collection and modification*, click **Data collection**.
2. Under *Advanced Settings to Allow for Ads Personalization*, expand the panel.
3. Click ⚙.
4. Turn off the switch for each geographical region you want to exclude, then click **Apply**.

In a Universal Analytics property

1. Sign in to Analytics.
2. Click **Admin**.
3. In the *Property* column, click **Tracking Info > Data Collection**.
4. Under *Advanced Settings to Allow for Ads Personalization*, expand the panel.
5. Click ⚙.
6. Turn off the switch for each geographical region you want to exclude, then click **Apply**.

To allow property data to be used to personalize ads

Follow the instructions above, but turn the switch on.

Control personalized advertising for a single Google Ads link

1. In **Admin**, under *Product links*, click **Google Ads links**.
2. Select the linked Google Ads account you want to edit.
3. Under *Enable Personalized Advertising*, turn the switch on or off.
4. Click **Save**.

Other ads-personalization controls

If you want to disable ads personalization for a single event or user property, and not for all events in a property, then there are other controls you may want to consider:

- Event and user-property controls in Analytics
- Event controls in Measurement Protocol

Give feedback about this article

Was this helpful? Yes No

Integrations

[GA4] Google Ads integration
[GA4] BigQuery Export integration
[GA4] Campaign Manager 360 integration via Floodlight
[GA4] Display & Video 360 integration
[GA4] Firebase integration
[GA4] Google Ad Manager integration
[GA4] Google Merchant Center integration
Salesforce Marketing Cloud integration
[GA4] Play integration
[GA4] Search Console integration
[GA4] Search Ads 360 integration
[GA4] Advanced settings to allow for ads personalization
[GA4] Exclude specific events and user-scoped custom dimensions from ads personalization
[GA4] Traffic-source dimensions, manual tagging, and auto-tagging
[GA4] Google AdSense Integration

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

[GA4] Data redaction

Configure web data streams to perform client-side text redaction of email addresses and user-defined URL Query Parameters.

The data-redaction feature helps to prevent the inadvertent collection of PII in the form of email addresses and URL query parameters. Data redaction uses text patterns to identify likely email addresses across all event parameters and the URL query parameters that are included as part of the event parameters page_location, page_referrer, page_path, link_url, video_url, and form_destination.

> **URL query parameter**: A key-value pair (e.g., `language=english`) that follows the question mark (?) at the end of a URL. For example, the value for the event parameter `page_location` might be the URL and query parameters `https://www.example.com/us?language=english&catalog=summer23`.

Data redaction evaluates events before they are collected to find and remove any text it understands as an email address or query parameter key-value pair. After removal of the offending text, data collection proceeds as expected.

You configure data redaction as one of the settings for a web data stream.

When you create a new property, email data redaction is on by default. For properties that you created before the release of this feature, you need to enable data redaction using the instructions below.

It's important to remember that while data redaction provides a powerful tool against inadvertently collecting PII, the ultimate responsibility for meeting regulatory requirements still lies with the entity collecting data. To further help you meet that responsibility, this feature lets you test your configuration to understand whether the text patterns you identify are redacted as expected (learn more). You can also use Debug View to monitor in real time how Analytics collects events from your site.

Some things to keep in mind

Data redaction is currently available only for web data streams.

Data redaction evaluates event data for email addresses on a best-effort basis.

Data redaction occurs client side after Analytics modifies or creates events (which also occurs client side) and before data is sent to Analytics.

Data redaction accepts percent-encoded URL query parameters, including Unicode characters accepted by browsers. For example, if you enter 名 as a query parameter, and enter https://www.example.com?名=john as a test URL, data redaction will interpret it as follows:

Test URL after you enter it	Redacted version
http://www.example.com/?%E5%90%8D=john	http://www.example.com/?%E5%90%8D=(redacted)

Data redaction may incorrectly interpret text as an email address and redact the text; for example, if the text includes "@" followed by a top-level domain name (e.g., example.com) it may be incorrectly removed.

Data redaction does not evaluate HTTP-header values, (for example referer, which may contain query parameters on older browsers).

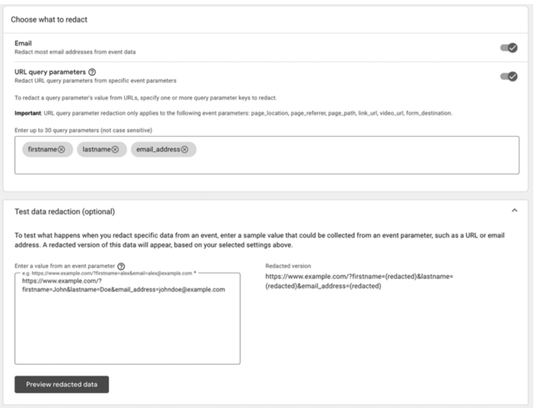
Data redaction won't prevent the collection of PII via Measurement Protocol or Data Import.

Configure data redaction

1. In **Admin**, under *Data collection and modification*, click **Data streams**.
2. Click the relevant web data stream.
3. In the *Events* section, click **Redact data**.
4. If you want to redact email addresses and/or URL query parameters, turn on the switch for each option.
5. If you choose to redact URL query parameters, enter a list of the query parameters you want to redact (e.g., firstname, lastname, email_address). Press **return/Enter** after each parameter.

Use the *Test data redaction* section to see how Analytics removes data. Analytics will test for the options you chose in Step 5 above.

1. Enter sample text containing an email address, or a URL that includes the query parameters you entered in Step 6 above along with sample values (e.g., `https://www.example.com/settings?firstname=John&lastname=Doe&email_address=johndoe@example.com`).
2. Click **Preview redacted data**.



Under *Redacted version*, you'll see an example of the data that Analytics would collect given your settings. For example, if your sample text is:

```
https://www.example.com/?firstname=John&lastname=Doe&email_address=johandoe@example.com
```

then the redacted version will be:

```
https://www.example.com/?firstname=(redacted)&lastname=(redacted)&email_address=(redacted)
```

Give feedback about this article

Was this helpful? Yes No

Data privacy and security
- Safeguarding your data
- Privacy controls in Google Analytics
- [GA4] Data redaction
- Introduction to user consent management
- [GA4] Verify and update consent settings in Google Analytics
- [GA4] Behavioral modeling for consent mode
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- Data Processing Terms
- We use our own products
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics
- Data sharing settings

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

[GA4] About events
[GA4] Automatically collected events
[GA4] Enhanced measurement events
[GA4] Recommended events
[GA4] Custom events
[GA4] Google Analytics event parameters

[GA4] Enhanced measurement events

Discover how to enable and disable enhanced measurement events and learn more about which parameters are collected for each event.

Enhanced measurement lets you measure interactions with your content by enabling options (events) in the Google Analytics interface. No code changes are required. When you enable these options for a web data stream, your Google Analytics tag starts sending events right away.

Before turning on the enhanced measurement feature, be sure you understand each option and what enhanced data will be collected. You can also turn off specific measurement options in settings.

> You're required to ensure that no personally identifiable information is collected.

Enable or disable enhanced measurement events

1. In **Admin**, under *Data collection and modification*, click **Data streams**.
2. Click the name of your data stream.
3. Under *Enhanced measurement*, slide the switch **On** to enable all options.
   Click ⚙ to edit individual options as needed.

If you use the Google tag on your website, you also need to make sure that each event is enabled for automatic event detection for your Google tag. By default, all event types are enabled. Learn more about your Google tag settings

Events measurement and parameters

The following table explains when events are triggered, and which parameters are collected for each event. You can find enhanced data about each triggered event in the Events report within the Engagement topic. Click the event name in the report for more information on the event.

To understand each event parameter listed below and how each parameter updates a dimension or metric in Google Analytics, see Google Analytics event parameters.

Measurement option / event	Triggered...	Parameters
Page views page_view	each time the page loads or the browser history state is changed by the active site This event is collected automatically. You cannot turn off collection. An advanced setting on this option controls whether the event is sent based on browser-history events. This measurement option listens for pushState, popState, and replaceState. The event populates the *Views* metric. The parameters populate the following dimensions: • *Page location* (from page_location) • *Page referrer* (from page_referrer)	page_location (page URL), page_referrer (previous page URL)
Scrolls scroll	the first time a user reaches the bottom of each page (i.e., when a 90% vertical depth becomes visible) The event populates the *Percent scrolled* dimension.	No parameters are collected
Outbound clicks click	each time a user clicks a link that leads away from the current domain By default, outbound click events will occur for all links leading away from the current domain. Links to domains configured for cross-domain measurement will not trigger outbound click events. The parameters populate the following dimensions: • *Link classes* (from link_classes) • *Link domain* (from link_domain) • *Link ID* (from link_id) • *Link URL* (from link_url) • *Outbound* (from outbound)	link_classes, link_domain, link_id, link_url, outbound (boolean)
Site search view_search_results	each time a user is presented with a search results page, as indicated by the presence of a URL query parameter By default, the event is triggered based on the presence of one of the following 5 query parameters in the URL: • q • s • search • query • keyword You can optionally configure this event to look for other URL query parameters. The search_term parameter populates the *Search term* dimension.	search_term, optionally 'q_<additional key>=""> (where <additional key>=""> matches an additional query parameter you specify to be collected under advanced settings). Note: This event only sends the unique_search_term parameter when it has a value of 1 (i.e. when the string is unique to that session).
Video engagement video_start video_progress video_complete	For YouTube embedded videos that have JS API support enabled, the following events are triggered: • video_start: when the video starts playing • video_progress: when the video progresses past 10%, 25%, 50%, and 75% duration time • video_complete: when the video ends The parameters populate the following dimensions: • *Video provider* (from video_provider) • *Video title* (from video_title) • *Video URL* (from video_url) • *Visible* (from visible)	video_current_time, video_duration, video_percent, video_provider, video_title, video_url, visible (boolean)
File downloads file_download	when a user clicks a link leading to a file (with a common file extension) of the following types: • document • text • executable • presentation • compressed file • video • audio File extensions that match the following regex will trigger the event: pdf|xlsx?|docx?|txt|rtf|csv|exe|key|pp(s|t|tx)|7z|pkg|rar|gz|zip|avi|mov|mp4|mpe?g|wmv|midi?|mp3|wav|wma The parameters populate the following dimensions: • *File extension* (from file_extension) • *File name* (from file_name) • *Link classes* (from link_classes) • *Link ID* (from link_id) • *Link text* (from link_text) • *Link URL* (from link_url)	file_extension, file_name, link_classes, link_id, link_text, link_url
Form interactions form_start form_submit	'form_start': the first time a user interacts with a form in a session 'form_submit': when the user submits a form You can use these two events to see how many users started to fill out a form and compare the information to users who submitted the form. Note: You can only use the parameters in your reports if you create custom dimensions for them.	form_start • form_id: HTML id attribute of the <form> DOM element • form_name: HTML name attribute of the <form> DOM element • form_destination: URL to which the form is being submitted form_submit • form_id: HTML id attribute of the <form> DOM element • form_name: HTML name attribute of the <form> DOM element • form_destination: URL to which the form is being submitted • form_submit_text: text of the submit button, if present

Give feedback about this article

Was this helpful? Yes No

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

©2024 Google - Privacy Policy - Terms of Service
English

[GA4] Collect granular location and device data

You have the option to enable/disable the collection of granular location-and-device data on a per-region basis. Analytics collects this data by default. If you disable this feature, then Analytics does not collect the following data:

- City
- Browser minor version
- Browser User-Agent string
- Device brand
- Device model
- Device name
- Operating system minor version
- Platform minor version
- Screen resolution

If you edit these settings and disable collection for a region, then Analytics maintains any historical data that you've collected (per your data-retention settings) but no additional data is collected from the time of the change forward.

1. In **Admin**, under *Data collection and modification*, click **Data retention**.
2. Turn on the switch for **Granular location and device data collection**.
3. When you turn the switch on, that data is collected in all regions. If you want to choose the regions in which the data is collected:
   a. In that same section, click .
   b. Next to *Granular location and device data collection is allowed in X of Y regions*, click .
   c. Turn the switch on or off for each region in which you want to allow or disallow data collection.
   d. Click **Apply.**

If you disable the collection of granular location and device data for a region, then modeled **key events** volume is significantly reduced for that region. Downstream key event modeling and reporting in linked Google Ads and Search Ads 360 accounts is also impacted.

Give feedback about this article

Was this helpful? Yes No

Help
Events and key events
Import data from external systems
Integrations
Measure ecommerce
Measure lead generation
[GA4] First-party data
[GA4] Measurement Protocol
[GA4] Collect granular location and device data
[GA4] Reporting identity

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

Set up your Google tag

The Google Tag powers the Google products you use with the data to measure the effectiveness of your website and app. This tag powers Google ads and measurement solutions, such as Google Ads and Google Analytics.

Your website and app visitors continue to evolve due to privacy, browser, and regulatory changes. Using the latest Google tag setup is important to help ensure you're getting the most accurate measurement.

This article shows you:

- Where to find your existing Google tag
- How to set up your Google tag using a template
- How to verify if your setup is working

How to use the Google Tag video tutorial

This video shows you how to set up your Google tag as a Google tag user. You can also set up the Google tag via Google Analytics, Google Ads, Campaign Manager 360, and Google Tag Manager.

For subtitles in your language, turn on YouTube captions. Select the settings icon at the bottom of the video player, then select "Subtitles/CC", and choose your language.

What is a tag ID and where to find it?

What is a Google tag?

Tag ID: A tag ID is an identifier that you or your page to track a given tag. It ends with a hyphen and a number, such as "AW-123456 or G-ABCDEF".

If you combine or split your tags, the new tag ID displayed in the tagging instructions changes your tag. You don't need to re-tag your site if this happens, as long as you have one of the tag IDs on a page. It will load the same tag. If you remove a destination, the tag ID will stop working.

Find your existing Google tag ID in Google Analytics or Google Ads:

- Open Google Analytics or Google Ads.
- Go to **Admin**.
- In **Data Streams**, click on a stream to see details.
  Result: Your screen shows the Google Analytics settings and the Google tag ID.

Campaign Manager 360 instructions

- Open Campaign Manager 360.
- Under "Floodlight", click **Google Tag** in left the Google tag settings.

Google Tag Manager instructions

Note: To use Google tag in Google Tag Manager, you need to manage a Google Ads, Analytics or Google tag in a container.

- Open Google Tag Manager.
- Click on the **Google tag** in your Google tags you have previously set up.

- Click on the tag to verify with the Google tag settings.

What is a destination and a destination ID?

What is a destination?

A destination is a Google measurement product account that shares configuration settings, and receives data from, a Google tag. You can add destinations to your Google tag to send data to Google products such as Google Ads or Google Analytics.

Currently, only Google Ads accounts and Google Ads where it Google Analytics 4 properties can be destinations.

What is a destination ID?

A destination ID is an identifier that represents the destination, i.e., the connected Google product, such as Google Ads or Google Analytics. The Google Tag uses the destination ID to look destination specific settings and to route events.

Set Google Ads, the destination ID is the same as the conversion tracking ID, or Google Analytics 4 property ID.

For Google Analytics, the destination ID is the same as your web data stream's Measurement ID, for example G-ABC.

Install the Google tag on your website

To accurately measure and use ads performance, you need to add the Google tag on every page of your website.

Install the Google tag on your site:

Tip: The Gtag.js and Google tag and Google Analytics, set up the Google tag to only one platform. You can add the same product tag on a destination in your Google tag.

If you have more complex measuring needs and want to manage third party tags as well, use Google Tag Manager to set up your Google tag.

Set up the Google tag from Google Ads instructions

Before you set up the Google tag, make sure you've set up conversion tracking for your website. On the Tags as a Google tag page, select the option that best describes your website. Follow the instructions to install the Google tag:

1. Use the Google tag tool on your website (Recommended)
2. Use a Google tag you already have
3. Install a Google tag

Use the Google tag found on your website (Recommended)

Use this tag (detected on your website) to complete setup without making changes to your site's code. Users for your account will be added as users on the tag. Learn more about Google tag permissions.

1. Click **Enable** to start your tag details.
2. Click **Finish**.

Note: As a precaution, we don't allow more one instance of your Google tag for each Google Ads account.

- When you set up an app tag, you need to configure your Google tag settings.
- You can launch Tag Assistant to test your tag event, action and data collection.

Use a Google tag you already have

This option shows whether the tag was detected on the site you entered. Choose a tag from the drop-down menu to add it to your account. Learn more about Google tags.

Note that if you can't see the traffic volume, your tag may be in the wrong account. If you choose a tag labeled "not detected", you may need to install it. Users for your account will be added as users on the tag. Learn more about Google tag permissions.

If you have admin access to the tag (new), you can choose "Add Google tag" if you're looking for, you may need the appropriate user permissions to make changes to the Google tag.

1. Click **Choose a tag** to discover.
   - If "Add Google tag" is shown, select it.
   - Or
   - Where the tag was detected.
   - Click **Add** to add the tag to the site you entered, you can choose a tag labeled "not detected" to complete setup without making changes to your site's code. If you choose a tag labeled "not detected", you may need to install it.
2. Select the Google tag you want to use, then click **Continue**.

Install a Google tag

Note: As a best practice, don't add more than one instance of your Google tag to each page of your website.

When you're set up your tag, you need to verify that your Google tag works.

Set up your Google tag From Google Analytics instructions

Here you set up your Google tag Google Analytics depends on if you're setting up a property for the first time or you are one of if you're adding a Google Analytics property to a site that already has universal Analytics.

If you're setting up Google Analytics for the first time

1. Select the Google Analytics account.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

If you're adding Google Analytics 4 properties to a site that already has universal Analytics

1. Select a Google Analytics account to create a new Google Analytics 4 property.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

If you're adding Google Analytics 4 properties to a site that already has universal Analytics

1. Select a Google Analytics account to create a new Google Analytics 4 property.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

Set up your Google tag From Google Ads instructions

Before you set up the Google tag, make sure you've set up conversion tracking for your website. On the Tags as a Google tag page, select the option that best describes your website. Follow the instructions to install the Google tag:

1. Use the Google tag tool on your website (Recommended)
2. Use a Google tag you already have
3. Install a Google tag

Use the Google tag found on your website (Recommended)

Use this tag (detected on your website) to complete setup without making changes to your site's code. Users for your account will be added as users on the tag. Learn more about Google tag permissions.

1. Click **Enable** to start your tag details.
2. Click **Finish**.

Note: As a precaution, we don't allow more one instance of your Google tag for each Google Ads account.

- When you set up an app tag, you need to configure your Google tag settings.
- You can launch Tag Assistant to test your tag event, action and data collection.

Use a Google tag you already have

This option shows whether the tag was detected on the site you entered. Choose a tag from the drop-down menu to add it to your account. Learn more about Google tags.

Note that if you can't see the traffic volume, your tag may be in the wrong account. If you choose a tag labeled "not detected", you may need to install it. Users for your account will be added as users on the tag. Learn more about Google tag permissions.

If you have admin access to the tag (new), you can choose "Add Google tag" if you're looking for, you may need the appropriate user permissions to make changes to the Google tag.

1. Click **Choose a tag** to discover.
   - If "Add Google tag" is shown, select it.
   - Or
   - Where the tag was detected.
   - Click **Add** to add the tag to the site you entered, you can choose a tag labeled "not detected" to complete setup without making changes to your site's code. If you choose a tag labeled "not detected", you may need to install it.
2. Select the Google tag you want to use, then click **Continue**.

Install a Google tag

Note: As a best practice, don't add more than one instance of your Google tag to each page of your website.

When you're set up your tag, you need to verify that your Google tag works.

Set up your Google tag From Google Analytics instructions

Here you set up your Google tag Google Analytics depends on if you're setting up a property for the first time or you are one of if you're adding a Google Analytics property to a site that already has universal Analytics.

If you're setting up Google Analytics for the first time

1. Select the Google Analytics account.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

If you're adding Google Analytics 4 properties to a site that already has universal Analytics

1. Select a Google Analytics account to create a new Google Analytics 4 property.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

If you're adding Google Analytics 4 properties to a site that already has universal Analytics

1. Select a Google Analytics account to create a new Google Analytics 4 property.
2. Enter a name.
3. Scroll up to the "Property" column, use the dropdown selector to select the property that is created. Use the name for what you want to set up your Google tag.
4. Click **Create** to create the Google tag.
5. Click the drop-down that you want to tag.
6. Under "Google tag", click **Configure Google tag**.
7. Click **Add** to add the tag to the site.

Set up your Properties

User properties are attributes that describe groups of your user base, such as their language preference or geographic locations. You can use user properties to define audiences.

To activate, you can set a user property under Customize > Events > Define, which also can be used to build user's favorite feed. You can use the Data API to segment users by favorite feed.

Google Analytics automatically collects some user dimensions so you don't have to define user properties for them. You can set up to 25 additional user properties for your Google Analytics 4 property.

To measure custom user properties you need to create a new **Google Tag Event** and configure the **Google Tag** to send it as a **User Property**.

1. **Save** your Google tag.
2. Go to **Analytics**.
3. Go to **Admin**.
4. Under **Property**, click **Data Streams**.
5. Select the Google tag stream you want to connect to.
6. Under **Tagging**, click **Configure tag settings**.
7. Under **Tagging**, click **Manage connected sites**.
8. Under **Connected site tags**, click **Add**.
9. Select the Google tag you want to connect to.
10. Click **Save**.

Note: Your configuration parameters should look like this:

Set up user properties

Google Analytics 4 properties

Google Tag Manager

Google Ads

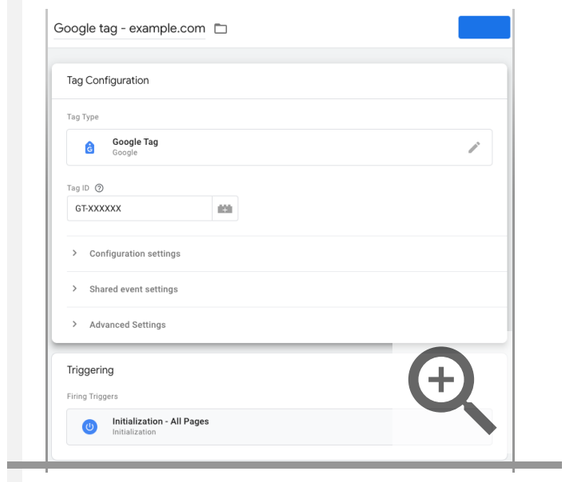
Google Ads and Google Analytics

Google Ads and Google Analytics

Google Ads and Google Analytics

Result

Your tag configuration should look like this:



Step 3: Publish the container

To update your website with the latest changes, click the **Submit** button at the top right.

Result

When you've set up your tag, verify that your Google tag works.

To set up more tags in Tag Manager, see your guide to Google Tag Manager.

Verify your tag sends data

1. Open Google Tag Assistant
2. Enter your site's URL.
3. Tag Assistant shows you all detected tags at the top. Check if your **Google tag** is showing up.
4. In the **Summary** tab, check if the tag sent any events.
   - ✅ Your Google tag is set up correctly when it records and dispatches events.
   - ❌ If you don't see your Google tag or it doesn't collect requests, see the sections below for more guidance.

Remember to set up the Google tag on every website that should send data. To check where your Google tag has been found, access the tag coverage summary.

No tag found

If Tag Assistant didn't find your Google tag, make sure that:

- You're adding the correct measurement ID
- Your code is live. You can use your browser's developer tools to see what code has been loaded.

Destination doesn't receive data

If Tag Assistant is showing that your Google tag is on your page, but you still don't see any data, your Google tag might not be connected to a destination.

In that case, you will be notified when you open the Google tag page. You can choose to connect the destination to an existing Google tag or to create a new Google tag.

Next steps

Once you've set up your Google tag, make sure you configure it to send the data you need.

Configure your Google tag settings →

Related links

- About the Google tag
- Manage your Google tag
- Manage Google tag users

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign in

Help guide
Help guide
Hi, I'm a **digital support assistant**. Chat with me to find answers and solve account issues.
Let's chat

©2024 Google - Privacy Policy - Terms of Service
English

Set up enhanced conversions for web using the Google tag

Enhanced conversions for web is a feature that can improve the accuracy of your conversion measurement. It supplements your existing conversion tags by sending hashed first-party conversion data from websites in a privacy-safe way. This feature uses a secure one-way hashing algorithm called SHA256 on your first-party customer data, such as email addresses, before sending it to Google. Enhanced conversions for web can help you measure more ad clicks and attribute your advertising conversions to ad clicks in Google Ads.

This article describes how to set up enhanced conversions for web using the Google tag. You can also set up enhanced conversions for web with Google Tag Manager or set up enhanced conversions for web with Google Ads API.

Note: Conversions measured by importing Google Analytics goals aren't supported for enhanced conversions. If you use the Google Analytics Conversion Tracking Code setting as a new Google Ads conversion action with the Google tag or Google Tag Manager

Before you begin

Review the following requirements before starting setup:

- Know the conversion page URL where the conversion tag fires (such as the confirmation page URL) and the conversion event trigger (for example, a button click or a page view).
- This implementation requires knowledge of how conversion tracking is set up on your website and tracks code changes, so make sure you're able to speak with your development team as needed.
- Ensure that you've reviewed and confirmed that you can collect the required conversion Customer data policies in Google Ads (view steps on this below, under "Instructions").
- If you set up conversion using URL, you can only set up enhanced conversions using the JavaScript or CSS selector options or automatic enhanced conversions.
- About 30 days after implementing enhanced conversions successfully, you'll be able to see the impact results in your conversion action table. Learn more about Enhanced conversions for web impact results.

Instructions

Note: The instructions below are part of the new design for the Google Ads user experience. To use the previous design, click the "Appearance" icon, and select **Use previous design**. If you're using the previous version of Google Ads, review the Quick reference map or use the Search bar in the top navigation panel of Google Ads to find the page you're searching for.

1. In your Google Ads account, click the **Goals** icon.
2. Click the **Conversions** drop down in the section menu.
3. Click **Settings** >.
4. Expand the "Enhanced conversions" section.
5. Check "Turn on enhanced conversions for web".
6. Review compliance statement. To enable enhanced conversions you must confirm that you'll comply with our policies and that the Google Ads Processing Terms is apply to your use of enhanced conversions. Click **Agree and continue** to acknowledge your acceptance of those terms.
7. Click the dropdown to choose a method for setting up and managing user provided data. Select "Google tag".
   Note: If you send Google enhanced conversions data in a way that's different from what you've already selected in Google Ads, that data may not be processed. For example, if you select "Google tag" and try to send data through Google Ads API, the data sent through API won't be processed.
8. If you're not sure which tagging method to select, click **Which method should I use?** Enter your website domain and click **Check URL** to view suggestions.
9. If you see a message stating that "your site may still collect user-provided data from your website" then you can optionally click **Save** to complete your setup.
   If you don't see the message above, or if you'd like to learn about other methods for collecting user-provided data, click **Next**.
10. On the tag details screen, you can decide how you'd like to capture user provided data in your tag:
    - **Automatically detect user-provided data**: Automatically inspect the page for strings that match a pattern for the configured page types. This method requires minimal effort and works well for most advertisers. For more control, consider adding a code snippet on your website or specifying CSS selectors or JavaScript variables. You can specify CSS selectors or JavaScript variables when automatic detection is turned on by clicking "add exclusions".
    - **Specify CSS selectors or JavaScript variables**: Manually specify CSS selectors or JavaScript variables on your page that contain relevant user provided data. If you'd like to use this method, select this option and follow the instructions below.
    - **Add a code snippet to your website**: Add a code snippet on your website that sends hashed customer data for matching. This method improves the accuracy of enhanced conversions because it allows you to send customer data from more ad clicks to improve your conversion tag flow. If you use this method you'll also have to select a checkbox under "Tag details" "will automatically process any user provided data you send on through a code snippet" if you do. You can use a combination of options. For example, you can select "Automatically detect user provided data" to apply automatic detection across all your conversion actions and then add a code snippet for specific conversion events of your choosing. Data provided through a code snippet is prioritized over automatically detected data. See the instructions below in "Add a code snippet to your website".
11. Click **Save**.
12. After you complete setup, validate your implementation to make sure enhanced conversion is set up correctly. After about 30 days you'll be able to see the impact of enhanced conversions on your reporting. Learn more about Enhanced conversions for web impact results.

Note: If you use either the automatic method or the CSS selector / Javascript variable method, Google will by default use an ads cookie to collect hashed, first party customer data on your behalf and process it for enhanced conversions. If you don't want Google to collect and process this data, implement Consent Mode, the ads cookie will be subject to the ad storage consent status of the Consent Mode feature, when implemented. You can disable this feature at any time by clicking the "Disable" button in the settings of your account, clicking "Google tags", and switching off "Form interactions" in your tag configuration.

Add a code snippet to your website

Before following the instructions below, make sure you've completed the steps in set up enhanced conversions and that you've selected "Google tag" as your data source.

Identify and define your enhanced conversions fields

Ensure that fields for customer email, address, and phone number are available on the conversion page where the Google tag fires. This will likely be the case on conversion pages for purchases, sign-ups, and other similar conversion types, which often require customer data. If you're unsure which page this is, you should contact your developer.

Note: At least one of the following fields must be provided:
- Email (preferred)
- Address (First name, last name, postal code, and country are required. You can optionally provide street address, city, and region as additional match keys.
- A phone number can also be provided along with an email or full name and address

You can either send unhashed data, which Google will normalize and hash before the data reaches the servers, or normalized and hashed data. If you decide to send normalized and hashed data, follow the below instructions.

For normalization:
- Remove leading or trailing whitespaces.
- Convert the text to lowercase.
- Format phone numbers according to the E.164 standard ↗.

For hash:
- Use hex SHA256.

The table below lists more information about the fields you can define. The "Key Name" column indicates how they'll be referenced in the enhanced conversions HTML snippet, which is created in the next step. Note, all data should be passed as String types.

Data Field	Key Name	Description
Email address	email	User email. Example: "jane@example.com"
	sha256_email_address	Hashed user email. Example: "a8a5f24f9934f2f5c06e5a5d6d3d6d1f3d6c3f"
Phone number	phone_number	User phone number. Must be in E.164 format ↗, with digits including country code (+ prefix and country code prepended), or spaces. Example: "+15123124567"
	sha256_phone_number	Hashed user phone number. Example: "e9c0ee4c77f4c9b1f8229f4b6e53d8cec4ce4d0C"
First name	address.first_name	User first name. Example: "John"
	address.sha256_first_name	Hashed user first name. Example: "9ed9d2f29c26b4c1c3332f24f7fc72a8f2f2332ee0
Surname	address.last_name	User last name. Example: "Doe"
	address.sha256_last_name	Hashed user last name. Example: "7f9a95ca2f4f9e2fb7f4f24f3f383b6e5f2f0a1b2
Street address	address.street	User street address. Example: "123 Main Rd"
City	address.city	User city name. Example: "Southampton"
Region	address.region	User province, state, or region. Example: "Hampshire"
Postal code	address.postal_code	User post code. Example: "SO99 1BX"
Country	address.country	User country code. Example: "UK". Use 2 letter count ry alpha 2 standard.

Note: You'll need to make sure the customer data is available when the conversion tag fires. If the user information is collected on a previous page, you'll need to make sure it's available in your code on the conversion page to configure it in this script.

Implement the enhanced conversions script

Configure and add the following script on your conversion page where the Google Ads event snippet is installed. Ensure that you update variable names below to match the variable names for those attributes on your web page.

For example, if you store email in a variable named "email_address" then the variable should be edited to reflect that (for example, where it says yourUserEmailArray).

Note: You can also hardcode the field with a string or use a function instead of using variables.

```
// implement
<script>
gtag('set', 'user_data', {
"email": [yourEmailVariable],
// Optional: If using additional data, ensure you are storing the user's
email data. In the same for the other variables below. Make sure
the values aren't hashed.
"phone_number": [yourPhoneVariable],
"address": [
{"first_name": [yourFirstNameVariable],
"last_name": [yourLastNameVariable],
"street": [yourStreetAddressVariable],
"city":[yourCityVariable],
"region": [yourRegionVariable],
"postal_code": [yourPostalCodeVariable],
"country": [yourCountryVariable]
}
]});
</script>
```

The phone number must be in E.164 format ↗, which means it must be 11 digits including a plus sign (+) prefix and country code with no dashes, parentheses, or spaces.

If you've doesn't collect one of the above fields, remove the field entirely rather than leaving it empty. For example, a website that only collects emails and phone numbers would look like this:

```
// implement
<script>
gtag('set', 'user_data', {
"email": [ yourEmailVariable ],
"phone_number": [ yourPhoneVariable ]
});
</script>
```

Note: At least one of the following fields must be provided:
- Email (preferred)
- Address - For address, first name, last name, postal code, and country are required. You can optionally provide street address, city, and region as additional match keys.
- Phone number (must be provided in conjunction with email, or full name and address)

Multiple values

Developers can optionally provide multiple values (up to 5 for phone and email and 2 for address) by using an array value rather than a string. If you capture more than one value, providing this will increase the likelihood of a match. Check out the following example:

```
<script>
gtag('set', 'user_data', {
"email": [yourEmailVariable1, yourEmailVariable2],
"phone_number": [yourPhoneVariable1, yourPhoneVariable2],
"address": [
{"first_name": [yourFirstNameVariable],"last_name:
[yourLastNameVariable], street: [yourStreetAddressVariable], city:
[yourCityVariable], region: [yourRegionVariable], postal_code:
[yourPostalCodeVariable],
{first_name: [yourFirstNameVariable],last_name:
[yourLastNameVariable], street: [yourStreetAddressVariable], city:
[yourCityVariable], region: [yourRegionVariable], postal_code:
[yourPostalCodeVariable]
]});
</script>
```

Configure your conversion page Google tag

Specify CSS selectors or Javascript variables

Before following the instructions below, make sure you've completed the steps in set up enhanced conversions and that you've selected "Google tag" as your data source. Also make sure you've selected "Specify CSS selectors or Javascript variables" as your implementation method.

Find enhanced conversions fields on your conversion page

1. Using the Chrome browser in a separate tab from your Google Ads account, navigate to your conversion page. If you're unsure which page this is, you should contact your developer.
2. Identify any customer data that's displayed on the page that you wish to send to Google Ads. For example, if you're using a thank you message and include a customer email address after a purchase.
   Note: At least one of the following fields must be provided for enhanced conversions to work properly:
   - Email (preferred)
   - Full name and address (first name, last name, street address, city, region, postal code, country)
   - Optional: A phone number can also be provided along with an email or full name and address (but not by itself)
3. Once you've identified the customer data on the page, you'll now need to follow the next step to loop the CSS Selectors or Javascript variables under those keys into Google Ads.

Identify enhanced conversions CSS Selectors and input into Google Ads

1. Follow the instructions to enable enhanced conversions and select "Specify CSS selectors or Javascript variables".
2. Click **Customize** to reveal a screen with fields where you can specify CSS selectors for each of your desired data types.
3. Check the box for each piece of customer data you plan to implement (for example: email, name and address, and phone).
4. Select **Javascript or CSS Selector**.
   Note: If you're using Javascript variables, it's likely easiest to ask your developer which variable is related to these fields. If you're using CSS Selectors, you can follow the steps below.
5. In a separate tab, navigate to your conversion page.
6. On your conversion page, when you've found the corresponding customer data you want to send with enhanced conversions, use your mouse to right-click on top of it and select Inspect.
7. If you're inputting the CSS selector for email in Google Ads, make sure you right click the email address displayed on your conversion page.
   This will open a window with the HTML code behind your Chrome browser.
8. Within the source code presented in the Chrome Developer Tools page, a portion of the code will be highlighted. This highlighted code is the portion which includes the CSS Selectors for the customer data you right clicked in Step 2 of this section.
9. Hover your mouse over the highlighted code and right-click it.
10. Scroll down to Copy and then choose Selector.
11. Paste that text in the corresponding fields in Google Ads (on your other tab). For reference, it should look something similar to but not exactly like this:
    `tr# > div:nth-child(2) > div.AfDbef > div.XMnHqb > div > div.w6Ocb > span.Text`
12. Complete steps 6-12 of this section for each different customer data type (email, name and address, and so on).
13. In Google Ads, click **Save**.

Validate your implementation

To verify if your enhanced conversions implementation is working correctly, navigate to your conversion page and then complete a test conversion to do this), and follow these steps. It's best practice to do this immediately after implementing enhanced conversions so any changes can be made if it's not working.

Validate your implementation using Chrome Developer Tools

1. Right-click on your web page.
2. Select **Inspect**.
3. Select the Network tab.
4. Enter "google" in the search bar.
5. Find the network request that's going to "googleadservices.com/pagead/conversion" (or "google.com/pagead/1p-conversion" on some browsers).
6. Click the Payload tab to view the list of query string parameters.
7. Look for a parameter "em" with a hashed string as the value. The value should start with "ko.1" followed by a long string of characters. If you see the "em" parameter, this means that the enhanced conversions tag is picking up and hashing the `enhanced_conversion_data` object.

Note: If you see the "em" parameter but you only see "ko.1" with without a long hashed string following it then you're sending the enhanced conversions parameter but it's empty. This may happen if your tag's data layer isn't available at the time of conversion.

After 72 hours, review the Diagnostics report to confirm your implementation

About 72 hours after implementing enhanced conversions, you'll be able to view the tag diagnostics report in Google Ads, which you can use to validate that your implementation is working properly. To get there:

1. In your Google Ads account, click the **Goals** icon.
2. Click the **Conversions** drop down in the section menu.
3. Click the conversion action that has enhanced conversions enabled.
4. Select **Diagnostics** from the page menu at the top. You'll be able to see your conversion action's tag diagnostics report and the metrics for your enhanced conversions in each section.
5. Review the various health checks to make sure everything is working as expected.
6. If the tag diagnostics report notifies you that something may be wrong, follow the instructions in the notification and the Help Center to troubleshoot.

Turn off enhanced conversions

Note: The instructions below are part of the new design for the Google Ads user experience. To use the previous design, click the "Appearance" icon, and select **Use previous design**. If you're using the previous version of Google Ads, review the Quick reference map or use the Search bar in the top navigation panel of Google Ads to find the page you're searching for.

To turn off enhanced conversions at the account level, follow the steps below:

1. In your Google Ads account, click the **Goals** icon.
2. Click the **Conversions** drop down in the section menu.
3. Select the conversion action you want to disable enhanced conversions for.
4. Click **Settings** >.
5. Expand the "Enhanced conversions" section.
6. Uncheck the checkbox next to Enable enhanced conversions.
7. Click **Save**.

To turn off enhanced conversions at the conversion action level, follow the steps below:

1. In your Google Ads account, click the **Goals** icon.
2. Click the **Conversions** drop down in the section menu.
3. Select the conversion action you want to disable enhanced conversions for.
4. Click **Settings** >.
5. Expand the "Enhanced conversions" section.
6. Uncheck the checkbox next to Enable enhanced conversions.
7. Click **Save**.

Note: If you turn off your enhanced conversions you won't be able to use them for bidding or reporting. However, turning them off will not affect your existing conversion data.

Give feedback about this article

Was this helpful? Yes No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign In

Data use across certain Google services in the European Economic Area (EEA)

As a result of the Digital Markets Act (DMA), starting March 2024 you will have new choices for how your data may be shared across certain Google services if you reside in the European Economic Area (EEA).

Linking Google services

Currently, personal data regarding your interactions with a given Google service may be shared across Google services for the purposes described in our Privacy Policy and depending on the previous choices you've made about your privacy settings.

Starting March 2024, Google will need your consent to link certain services if you want them to continue to share data with each other and with other Google services as they do today. For example, linking Google services might give you more personalized content and ads, depending on your settings.

Which Google services are impacted

The following Google services will require consent to share data for certain purposes, including showing ads:

- Search
- YouTube
- Ad services
- Google Play
- Google Shopping
- Google Maps

Other Google services not listed here may have different linking configurations that permit them to share data with each other for the purposes described in our Privacy Policy, depending on your settings.

What data is used

Personal data that is collected about your interaction with Google services can be shared across any linked services. This includes:

- Searches
- Videos you watch on YouTube
- Apps you install from Google Play
- Associated information, like your location and device info
- All other types of information described in our Privacy Policy

How we use this data

Google uses data shared across linked services for all the purposes that are set out in our Privacy Policy, including:

- Providing personalized services, including content and ads, depending on your privacy settings
- Maintaining or improving our services for everyone
- Understanding how people use our services to ensure and improve the performance of our services
- Performing other purposes described in our Privacy Policy

What won't be affected

The choices you make about linked services will not affect:

- The purposes for which we use data
- Your privacy settings, such as choices you made about personalizing Google services
- Aspects of service that don't involve sharing data

Your data from all Google services, regardless of whether they are linked, may still be shared across all services for certain purposes, like preventing fraud, protecting against spam and abuse, and complying with the law.

Additionally, when two or more Google services are offered together, your data may also be shared across those services to perform functions that rely on both of those services.

If you choose not to link any of the listed services, some features of those Google services that involve sharing data across Google services will be limited, but your services otherwise will not be affected. For example, if you have turned on personalization for a service through your privacy settings, but choose not to link it, that service will still be personalized, but based only on data from that service.

How to manage linked services

You can manage your choices, including selecting other Google services to link or withdrawing your consent to services being linked, in your Google Account. You can also manage other settings, like Web & App activity, YouTube History, and Personalized ads in your Google Account.

Using personal data from our advertising partners

When you interact with our advertising partners — websites, apps, and services that use Google advertising tools — you may share personal data with such businesses and advertisers, or companies working on their behalf. Our advertising partners may, subject to our EU user consent policy, share this data with Google services for advertising purposes. See our Privacy Policy for the types of data used by Google advertising services.

If you reside in the EEA, our advertising partners must have your consent to share your personal data with Google for personalized advertising and instances where cookies or local storage is used. Advertisers may use consent banners to gather your permissions for personal data use when you are on their websites or apps, or alternatively collect your consent in other ways, for example, an email signup.

Additionally, advertisers will have the ability to select specific Google services that can receive the personal data you consent to share with Google for advertising purposes. Once data from advertisers is collected and processed by the selected Google services, your respective Google service settings will apply.

Configure your Google tag settings

The Google tag lets you send data from your website to connected Google product destinations to help you understand the effectiveness of your website and ads. After you place the Google tag on your website, it sends to linked Google product destinations, such as Google Ads and Google Analytics. You can use a single Google tag implementation for all your products and accounts.

Before you configure the Google tag settings, make sure you set up your Google tag on every page on your website.

This article explains how you can configure your Google tag settings. You can also Manage your Google tag by editing your Google tag name, combining Google tags, or adding or removing destinations.

Open the Google tag settings

Google Ads instructions

Open the Google tag settings ☰.

Google Analytics instructions

1. Open Google Analytics ☰.
2. Go to the **Admin** screen.
3. In **Data Streams**, click on a stream to see details.
   Result: Your screen should show you the Google Analytics settings and the Google tag settings.
   1. Main stream details

Campaign Manager 360 instructions

1. Open Campaign Manager 360.
2. Under "Floodlight", click **Google Tag** to edit the Google tag settings.

Google Tag Manager instructions

Note: To see Google tag IDs in Google Tag Manager, you need to manage a Google Ads, Analytics or Google tag in a container.

1. Open Google Tag Manager ☰.
2. Click on the tab **Google tag** to see Google tags you have previously set up.

3. Click on the tag name to edit the Google tag settings.

Configure your Google tag settings

When you are in your Google tag settings, click **Show all** to review all available settings.

Note: Tag settings affect the behavior of your Google tag and the data sent to configured destinations. Some settings may be more or less relevant for you depending on which products you use. You may choose to configure settings that are less relevant for your current setup of the Google tag. When you add new product destinations or their capabilities change, the settings will go into effect.

Configuration settings	Description	Relevant for Google Ads	Relevant for Google Analytics	Relevant for Campaign Manager 360
Manage automatic event detection	Configure which types of events your Google tag automatically detects and sends measurement in associated destinations.	Yes	Yes	Not Currently
Configure your domains	Specify a list of domains for cross-domain measurement.	Yes	Yes	Yes
Allow user-provided data collection	Configure whether your Google tag should allow user-provided data to be included in ad personalization and other destination products that support it.	Not Currently	Not Currently	Not Currently
Collect Universal Analytics events	Collect an event each time a gaq.push command event, timing, or exception call from Universal Analytics sources on your website.	Yes	Not Currently	Not Currently
Define internal traffic	Define IP addresses whose traffic should be marked as internal.	Yes	Not Currently	Not Currently
List unwanted referrals	Specify domains whose traffic should not be considered to be referrals.	Yes	Not Currently	Not Currently
Adjust session timeout	Set how long sessions can last.	Yes	Not Currently	Not Currently
Override cookie settings	Change how long cookies last and how they are updated.	Yes	Not Currently	Not Currently
Manage data use across Google services	Choose which Google services can receive consented data from end users in the European Economic Area (EEA) for advertising purposes.	Yes	Yes	Yes

Configure your Google tag settings

Manage automatic event detection

Select which types of events your Google tag should automatically detect for measurement in associated destinations. By default, all event types are turned on.

If you turn off automatic event detection, no products or accounts that use this Google tag will be able to receive associated data. You may want to consider turning off collection of these events in your destination instead.

By default, all event types are turned on. Click the switch to turn the following event types off:

- **Page views:** Detect a page view event each time a page loads. You can't disable this event type.
- **Page views on browser history change:** Detect a page view event each time the website changes the browser history state. This setting is useful for detecting page views in single page applications.
- **Scrolls:** Detect scroll events each time users reach to the bottom of the page.
- **Outbound clicks:** Detect an outbound click event each time a visitor clicks a link that leads them away from your domain(s). By default, outbound click events will occur for all domains separate from the current domain. Links to domains configured for cross-domain measurement (in the "Configure your domains" setting) will not trigger outbound click events.
- **Form interactions:** Detect a form interaction or form submission event each time a visitor interacts with a form on your site.
- **Video engagement:** Detect video play, video progress, and video complete events as visitors view embedded videos on your site. By default, video events will be automatically detected for YouTube videos embedded in your site with JS API support ☰ enabled.
- **File downloads:** Detect a file download event each time a link is clicked with a common document, compressed file, application, video, or audio extension.

Configure your domains

Specify all of your domains that use this tag. This list enables cross-domain measurement and further defines which links on your site do not trigger Outbound Click events when using automatic event detection.

- If you use the same Google tag across domains, they are automatically detected and listed in the Suggested Domains section. To accept a recommendation, click **Add**. To manually add a domain, click **Add condition** under include domains that match the following conditions:
  - Choose a match type.
  - Under Domain, enter the identifier for the domain you want to match (e.g., example.com).
  - Add each domain you want to include in cross-domain measurement.
- 2. When you've specified all the domains that use this tag, click **Save**.

The changes you make here could affect other Google tags loaded on the same page.

Verify that cross-domain measurement is working properly

Cross-domain measurement works by appending parameters to the URLs on your website. In rare cases, your web server might run into an error, such as returning a 5xx error response code or failing to start a download.

To verify cross-domain measurement works:

1. Open a page of your site that contains a link or a form that points to a domain you configured for cross-domain measurement.
2. Click the link or submit the form to navigate to the destination domain.
3. Verify that the page loads correctly.
4. Verify that the URL in the destination domain contains the linker parameter `_gl`. For example: `https://www.example.com/?_gl=1*abcdefg`.
5. If your website provides any downloads, navigate to a page with the linking parameter in the URL and start a download. Verify that the download starts successfully.

If you encounter an error, try Troubleshooting cross-domain measurement.

Allow user-provided data capabilities

User-provided data helps improve measurement and give you more insights with data that people provide to your website. Google will only use the data you share to provide you services, including technical support. Google will not share your data with others.

Destination product terms

No data will be collected by destination products if that data is disabled by that product's Terms of Service or if the terms required for collecting data from this feature aren't accepted.

- **Google Ads:** Google Ads Data Processing Terms ☰
- **Google Analytics:** Google Analytics Data Processing Terms ☰
- **Campaign Manager 360:** How Google uses Google Marketing Platform advertising product data ☰

Configuration

1. To control whether any destination products can receive data from this feature, enable or disable the **Allow user-provided data capabilities** option. Note: If you choose to turn off "User provided data," no products or accounts that use that Google tag will be able to receive data from this feature.
2. Choose how you want to include user-provided data. User-provided data will be hashed to keep it private and then sent along to your destination products that are configured to receive it with other event data. You can enable one or more configuration options:
   - **Automatic detection:** Automatically inspect the page for strings that match a pattern for email addresses.
   - **CSS and variable selectors:** Specify CSS selectors or JavaScript variables on your website.
   - **Manual via code:** Modify your Google tag to collect data on the account level. See Setting up enhanced conversions with the Google Tag.
3. Click **Save**.

Note: The use of this tag is subject to the terms governing the service where it is used.

Collect Universal Analytics events

Turn on the switch to collect an event each time a legacy gaq.push custom event ☰, timing, or exception call from Universal Analytics sources on your website.

Define internal traffic

Define IP addresses whose traffic should be marked with a custom traffic type identifier. Incoming traffic from matching IP addresses will have a `traffic_type` parameter appended with the selected value.

Tip: This feature can be used to mark internal traffic in coordination with settings in destination products, like Data filtering in Google Analytics.

1. Click **Create**.
2. In the top right corner, select the pencil icon ✎ to edit the configuration.
3. In the "Rule name" section, give your rule a descriptive name.
4. In the "traffic_type" section, choose the name of the `traffic_type` parameter. The default value is `internal`.
5. In the "IP address", select your match type and enter a value. If you don't know your IP address, click **What's my IP address?** ☰. Matching can be done on either one or IPv4 addresses. Ranges of IP addresses can be specified using CIDR notation, such as 192.0.2.0/24 or 2001:db8::/32. Learn more about CIDR notation ☰
6. Use distinct values to help you differentiate and filter different sets of traffic.
7. Click **Add conditions**. When you're done, click **Create**.

List unwanted referrals

Specify domains whose traffic should not be considered to be referrals. This feature will append the `ignore_referrer` parameter to events on pages where the traffic source matches the specified domains.

Tip: This feature can be used to specify referral traffic that you don't want to affect your measurement in destination products (for example, ignoring unwanted referrals in Google Analytics).

1. Select to ignore referrals that match any of the following conditions as traffic sources. You can select a match type that:
   a. Contains
   b. Begins with
   c. Ends with
   d. Exactly matches
   e. Matches RegEx
2. Click **Add conditions**. When you're done, click **Create**.

Adjust session timeout

Products like Google Analytics 4 that receive data from the Google tag use sessions to measure periods of user activity on websites where the tag is installed. Use this feature to change how long sessions should last by adjusting how long it takes before sessions expire due to inactivity or become engaged sessions.

1. **Adjust session timeout** by selecting the hours and minutes. A session is initiated when a webpage is loaded. A session ends after a period of inactivity on the page of the user. The default timeout is 30 minutes but can be adjusted here.
   - Engagement is measured differently than inactivity on a webpage. A session becomes an "engaged session" if it lasts longer than a certain amount of time. The default threshold for engagement time is 10 seconds but can be adjusted here. Learn more about sessions
2. Click **Save**.

Override cookie settings

Change how long cookies last and how they are updated. You can override your Google tag first-party cookie settings. Learn more about cookies and user identification ☰

Google tags use first-party cookies for various purposes. These cookies have default expiration and update settings, but you can customize these settings by overriding them.

1. Click the checkbox to override the default expiration and update settings of cookies used for analytics purposes.
2. Set how long before analytics cookies expire. Cookie expiration time will be the current time when the cookie is set or updated plus the value of this field. Learn more about cookie expiration ☰
3. Under "Cookie update" choose:
   a. **Set cookie expiration time relative to the most recent visit:** By default, each time a user visits your site, your Google tags update the expiration date of associated cookies, extending the cookie lifetime relative to the user's most recent visit.
   b. **Set cookie expiration time relative to first visit:** You can optionally set your cookie expiration time relative to your users' first visit, in which case the expiration is set once and never updated. Learn more about cookie update ☰
4. Click **Save**.

Manage default consent settings for data collection

Adding users for their consent to collect data is an integral part of measurement. Why does managing user consent matter?

When these settings are for

The Google tag settings let you set a default consent setting if you:

- Don't use consent mode
- Prevent your Google tags from loading until a user interacts with your consent banner

If you already use consent mode, the Google tag default settings aren't applied to your tags. Instead:

- If you use consent mode and don't engage in personalized advertising, you don't need to take any action.
- If you use consent mode and rely on ad personalization capabilities, implement consent mode version 2.

Set a default consent state

To set a default consent state:

- If your website or app operates independently of user consent requirements, select **My business sends data to Google independent from user consent choices**.
- If you obtain user consent and only send data after receiving consent, for example, by blocking tags, select **My business confirms that user consent has been granted before data is sent to Google**.
- If you upload data from other sources to Google, you need to label that data with user consent as well. Other sources include:
  - Google's store sales direct solution
  - Offline Conversion Import
  - File upload solutions, for example, spreadsheet uploads
  - a CRM integration

If the data uploads don't contain consent labels but you only gather them after a user consented, check **Apply this setting to additional data sources**.

Manage data use across Google services

You can decide which Google services can receive consented end user data. For optimal measurement, make sure that all Google services receive consented end user data.

If your business requires you to restrict data sharing across Google services, choose **Select Google services**. Select all Google services that are allowed to receive user-consented data for measurement and personalization.

Ensure that you declare in your consent banner which Google services receive user-consented data.

When you've configured your Google tag settings, you can manage your Google tag from the "Admin" tab.

Related links

- About the Google tag
- Set up the Google tag
- Google tag management

Give feedback about this article

Was this helpful?
Yes
No

Need more help?
Sign in for additional support options to quickly solve your issue
Sign In

Achieve your advertising goals today!
Attend our Performance Max Masterclass, a livestream workshop led by Google Partner industry and Google ads Pillar experts.
Register now