COOKIE CONSENT

Introduction to Cookie Consent Management
Why do you need Cookie Compliance?

Cookies are pieces of code that pass your consumers' data among web servers, browsers, and websites to help tailor the digital experience. Cookies can achieve this by collecting the consumers' personal information from their browsing behaviors. The personal information may include the following.

- Names

- Home address and phone numbers

- Credit card numbers, passport numbers, and other document numbers

- Employment records

- Online shopping history

- Email-id and IP address

To ensure transparency of the above process, recently some popular regulations like CCPA in California, GDPR in the European Union, LGPD in Brazil, and CNIL in France came into effect strictly. So, we provide an application for building a cookie consent banner and managing the cookie consent records to comply with these regulations. The Cookie Consent application also monitors the collection, usage, and sale of personal data of website users.

How to manage Cookie Consent?

Adzapier provides an application for Cookie Consent management that includes the following components.

- Cookie Scanner - An automatic cookie scanner scans all the cookies on your domain as well as subdomains and categorizes them into a list.

- Cookie Banner Configurator - You can configure a fully customized cookie banner with multilingual options for your website that shows the cookie information and the privacy policy of your organization.

- Cookie Consent Dashboard - An information panel for monitoring cookie consent activities including the opt-in and opt-out activities, domain and subdomain-wise data, and state/country-wise consent analytics.

- Consent Tracker - Helps the website publishers and admins to track the record of all consent details including opt-in, opt-out, user's geo-location, device ID, IP address, and so on.

Cookie Scan and Categorization

With your Adzapier Portal account, after successfully subscribing to a Cookie Consent plan, and assigning desired property under the plan to the subscription, you can now scan for cookies from the domain, and add cookies manually to the domain. Also, you can edit the details of existing cookies.
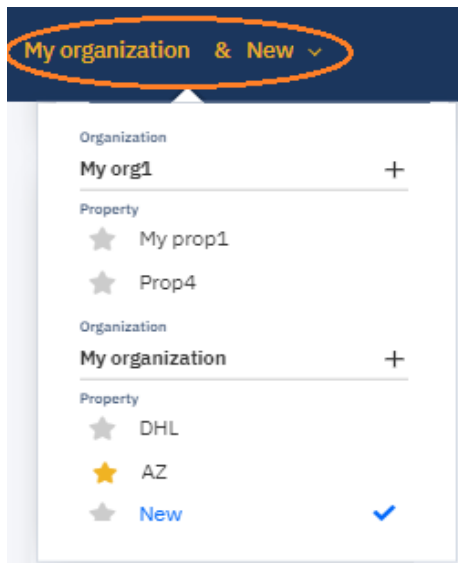
Cookie Scanning

You can scan your domain for cookies. The results of the scan will be obtained category-wise and the same will be fetched on the cookie category page. When you publish the cookies, the details of the cookies will be displayed category-wise to the domain users through the cookie consent banner.

The following example of a cookie banner shows how the user can view the cookie details category-wise through the cookie content banner.
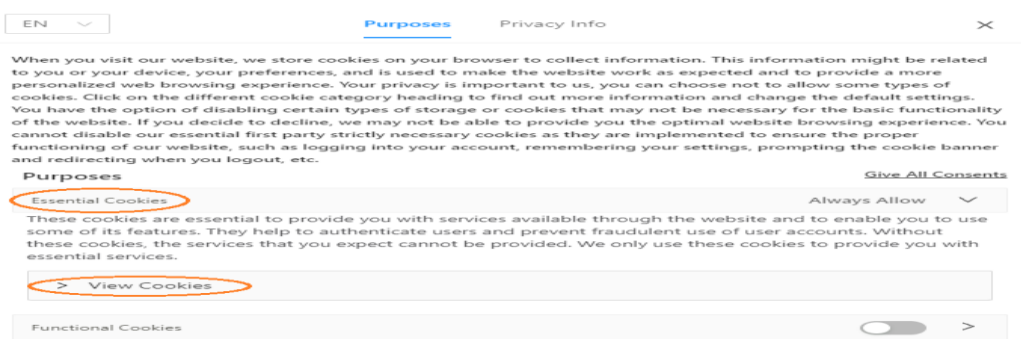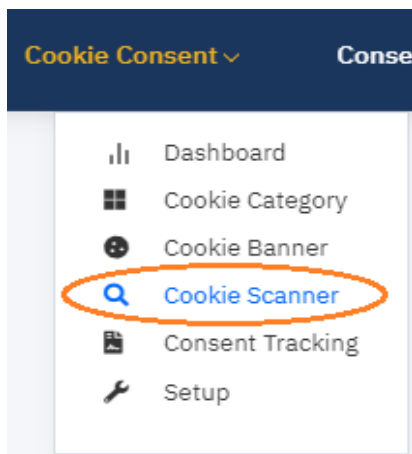
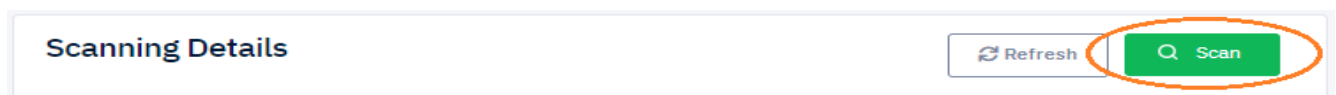Follow the steps to scan the domain for cookies.

1. On your account home page, in the menu bar, click the organization & property selector menu.

2. The list of organizations with the properties appears.

3. Select the property that you want to scan.
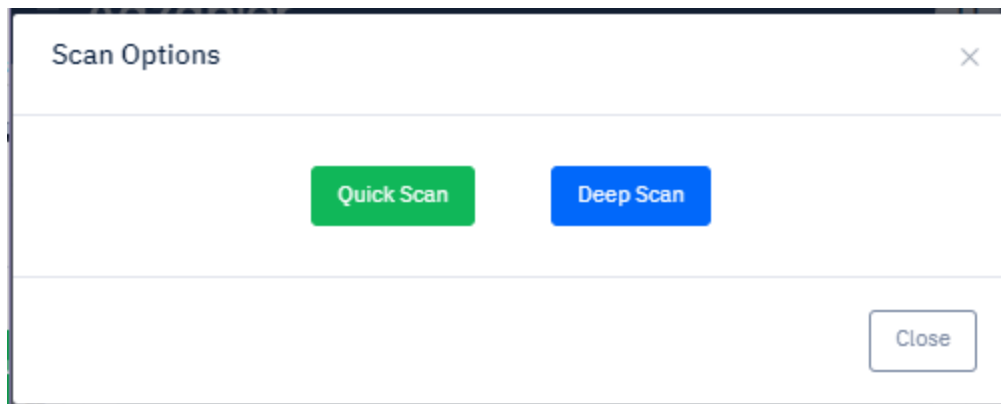
4. In the Cookie Consent menu, click Cookie Scanner.

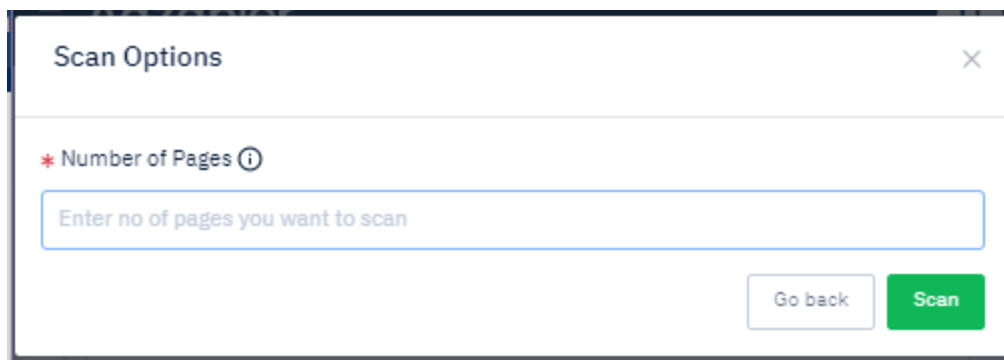The Scanning Details page appears.

5. Click Scan.

The Scan Options appear.

Scan Options   ✕

Quick Scan   Deep Scan

Close

Note: If your website has an authentication form, you can select Scan Behind Login. To learn about this feature, see Scan Behind Login.
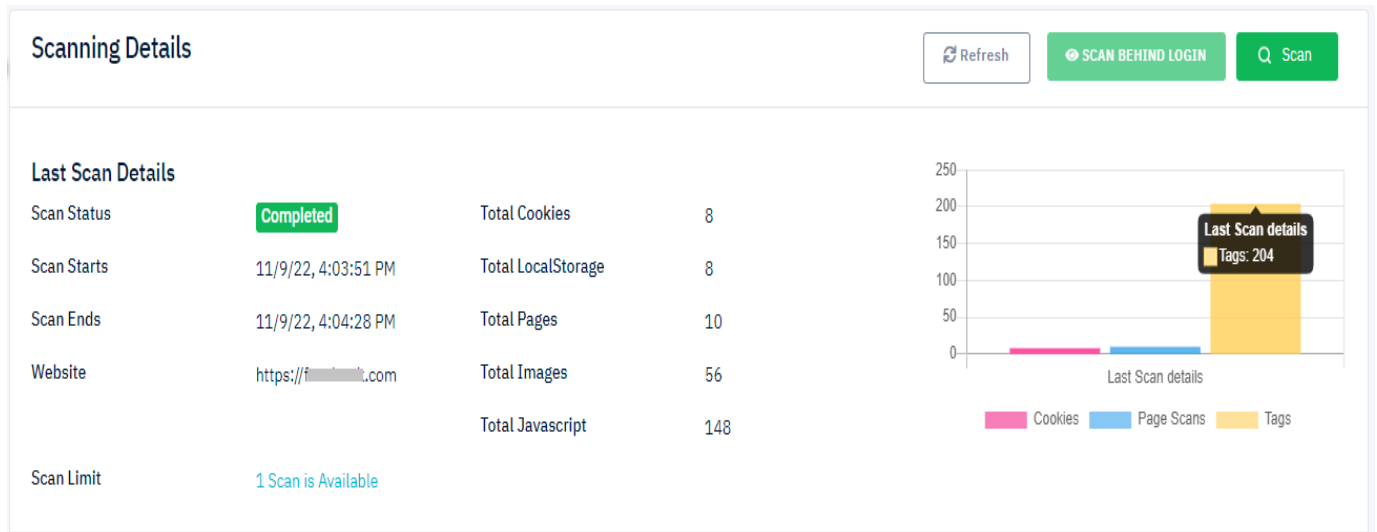
6. If you want to scan up to 10 pages of your domain, select Quick Scan.

Or if you want to scan more pages, select Deep Scan.

Scan Options   ✕

* Number of Pages ⓘ

Enter no of pages you want to scan

Go back   Scan

Enter the number of pages to be scanned and click Scan.

- The scan process starts.

- When the scan is in progress, it shows the Scan Status as "Running". Once the scan is completed, the status will show "Completed".

- Then the pie chart analytics of the scanned details also appear on the window.

Scanning Details

Refresh | **SCAN BEHIND LOGIN** | **Scan**

Last Scan Details

Scan Status	Completed	Total Cookies	8
Scan Starts	11/9/22, 4:03:51 PM	Total LocalStorage	8
Scan Ends	11/9/22, 4:04:28 PM	Total Pages	10
Website	https://f_____.com	Total Images	56
		Total Javascript	148
Scan Limit	1 Scan is Available		

Last Scan details
Tags: 204

Cookies ■ Page Scans ■ Tags

7. You can check the current and prior scan histories in the lower section of the page when the scan is finished.

Scans History

	ID	Requested By	Scan Type	Scan Start	Scan End	Scan Status	Total Cookies	Total LocalStorage	Total Images	Total JavaScript	Total Page Scan
>	43ec1c6f-46b2-4bdd-8efc-0818b3f513db	Snigdharani Behera	Manual	1/11/23, 6:47:36 PM	1/11/23, 6:48:51 PM	Completed	24	20	80	57	10
>	958bde21-f23d-4af7-b317-4ea6f1ec54a1	Snigdharani Behera	Manual	1/11/23, 6:25:36 PM	1/11/23, 6:26:42 PM	Completed	27	20	77	60	10
>	abdae91d-0949-475b-ac75-ab5ef1f3c733	Snigdharani Behera	Manual	12/15/22, 9:52:22 PM	12/15/22, 9:53:19 PM	Completed	2	0	92	45	10
>	bf50a43b-3edc-4bb8-91c5-983d6ab789c5	Snigdharani Behera	Manual	11/3/22, 5:30:02 PM	11/3/22, 5:30:57 PM	Completed	10	0			1

10 ∨   « ‹ 1 › »   Showing 1 to 4 of 4 entries

8. If your website contains Sub Domains, you can view the scan history of every Sub Domain by clicking the arrow on the left.

Scans History

	ID	Requested By	Scan Type	Scan Start	Scan End	Scan Status	Total Cookies	Total LocalStorage	Total Images	Total JavaScript	Total Page Scan
˅	43ec1c6f-46b2-4bdd-8efc-0818b3f513db	Snigdharani Behera	Manual	1/11/23, 6:47:36 PM	1/11/23, 6:48:51 PM	Completed	24	20	80	57	10

Sub Domain

Website	Requested By	Scan Type	Scan Start	Scan End	Scan Status	Total Cookies	Total LocalStorage	Total Images	Total JavaScript	Total Page Scan
https://suppor...	Snigdharani Behera	Manual	1/11/23, 6:47:36 PM	1/11/23, 6:47:58 PM	Completed	3	0	2	7	10

Cookie Categorization

1. Once the cookie scan is done, the cookies are categorized automatically. To view the cookies, go to the Cookie Category page.
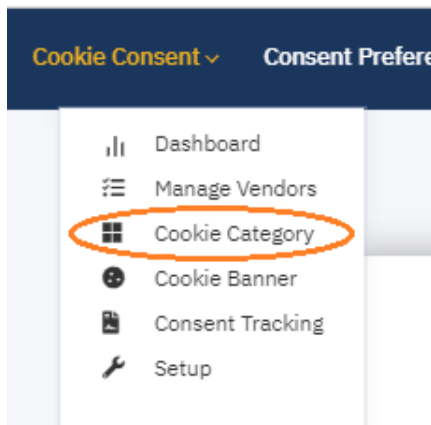
2. In the table of cookies, if you want to add more columns to the table, in the Choose Columns list, select any columns to be included.
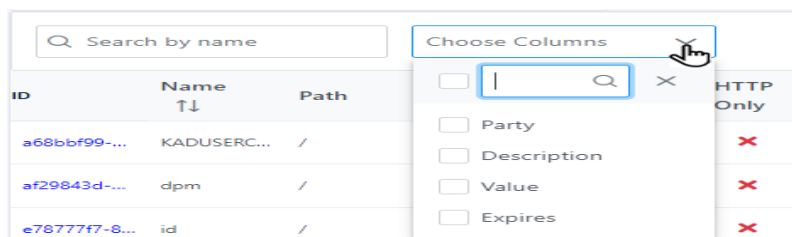
3. The cookie details from the scan results are added on this page with the following details.
    > Cookie ID - unique ID generated for each cookie
    > Cookie name
    > Path - the server path on which the cookie will be available
    > Category - any of the six categories
    > Domain - the website on which the cookie is available
    > Http Only - whether the cookie tagged as Http Only prevents client-side scripts from accessing data
    > Secure - whether the cookie flagged as Secured which may contain sensitive data
    > Website - domain or subdomain
    > Party - either first-party or third-party
    > Description of the cookie
    > Value of the cookie
    > Expires - the validity of the cookie

4. Enter the cookie name in the Search by name field to view any cookie details by its name.

5. To apply more search filters, click on the filter.
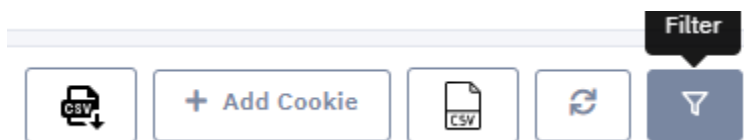
6. The filtering parameter pop-up will appear.

7. You can filter out the cookie details by Cookie Category, HTTP Only, and Secure Only.

8. After entering all parameters click Apply.

Note:

- This application scans for cookies from your domain and categorizes them automatically. Once you start the Scan, it takes a few minutes to complete the scan depending on how heavy the website is.

- The available number of scans is shown on the Scanning Details page.

Scanning Details

Last Scan Details

Scan Status	Completed	Total Cookies	8
Scan Starts	11/9/22, 4:03:51 PM	Total LocalStorage	8
Scan Ends	11/9/22, 4:04:28 PM	Total Pages	10
Website	https://f_____.com	Total Images	56
		Total Javascript	148
Scan Limit	1 Scan is Available		

- The limitation of the number of scans depends on the plan that you have subscribed to. For more details about the limitations, see the Adzapier Plans and Pricing.

- Suppose the limitation on the scan gets over and if you still want to scan, click Scan. The updated plan option popups then you can update the plan.

Add Cookie (Manually)

You can add a cookie manually to the domain.

1. Go to the Cookie Category page. Click Add Cookie.

Add cookie details manually
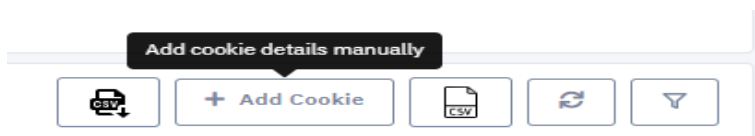
+ Add Cookie

2. Add Cookie details page will appear.

Add Cookie

✱Cookie Name

Enter cookie Name

✱ Category

✱ Domain

Enter Domain

✱ Path

Enter Path

✱ Party

◯ First-Party   ◯ Third-Party

✱ Description

Enter Description

✱ Value

Enter Value

Cancel   **Save**

3. Enter the Cookie Name, Domain, and Path.

4. In the Category box, select the purpose of the cookie.

5. Under Party type, select First Party or Third-Party.

6. Type any Description and any Value. You may enter any alphanumeric characters.

7. Click Save.

Note:

- The Cookie name can be found by checking the cookies via the browser.
- The Path of the server on which the cookie will be available.
- The Value is used for cookies that can create a different value per session.
- You can add more cookies in the same way by entering different details in each cookie.

Manage Cookies

You can edit or delete any existing cookies available on the property.

Go to Cookie Category. It shows the analytics of cookies and the list of cookies scanned from the domain and manually added cookies to the domain.

The analytics of cookies of the domain is shown using two pie charts, that is Cookies by Purpose and Cookies by Party type (First Party or Third-Party). When you hover over each slice of those pie charts, it shows the count of each cookie type.

Edit Cookie Details

1. Go to Cookie Category.

2. From the list of cookies, right to the cookie that you want to edit click 🖊

3. Edit Cookie Details page will appear.

4. Change any details and click Save.

Bulk Edit Cookies

1. Select the cookies you want to edit in bulk. Click Bulk Edit.

2. Bulk Edit Cookies pop-up appears. Select the fields you want to update.

3. Select the fields from the drop-down. You can select any field as per your requirement.

Bulk Edit Cookies

Bulk edit you wish to perform on the selected 4 cookies.

Select field(s) you want to save

☒ Cookie Category ☒ Domain ☒ Path ☒ Party ︿

☑ Cookie Category

☑ Domain

☑ Path

☑ Party

✳ Domain

Enter Domain

✳ Party
○ First-Party ○ Third-Party

Cancel   **Save**

4. Update Cookie Category, Domain, Path, and Party fields.

Bulk Edit Cookies

Bulk edit you wish to perform on the selected 4 cookies.

Select field(s) you want to save

☒ Cookie Category ☒ Domain ☒ Path ☒ Party ﹀

✳ Category

-- Disable --   ⌄

✳ Domain

Enter Domain

✳ Path

Enter Path

✳ Party
○ First-Party ○ Third-Party

Cancel   **Save**

5. Click Save.

Delete a Cookie

1. Go to Cookie Category, from the list of cookies, right to the cookie that you want to

    delete click

2. Click Yes to confirm.

Export Cookie Details

You can export the cookie details of a property as a CSV file.

- Go to Cookie Category and click on Export Cookie.
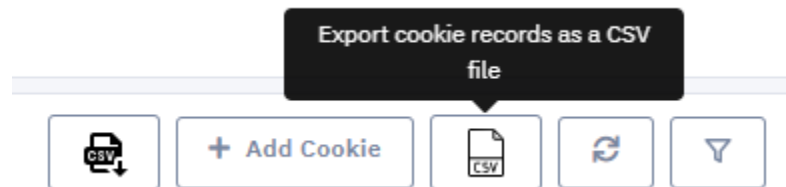
- A CSV file will be downloaded containing all the cookie details as you view in the list of the cookie details.

Import Cookies from a CSV File

- Go to Cookie Category and click on Import Cookies.
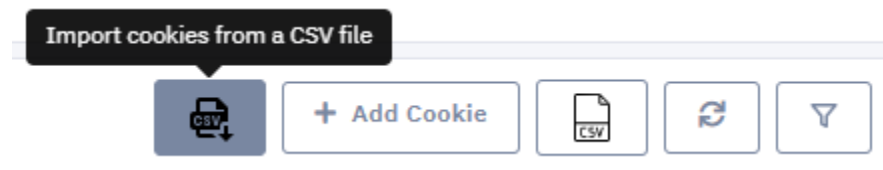
- Then the following pop-up will appear.

- Click on Click to download sample Cookie CSV file to download a sample CSV file for your reference.
- Then click on the Browse button to choose a CSV file from your device and then click on Import.
- You can view the cookies imported from the CSV file in the cookie category table.

Configure Cookie Banner

With your Adzapier portal account, after scanning your website for cookies or adding the cookie details manually, you can now configure your cookie consent banner to be displayed on your domain.

You can configure your cookie banner concerning the following three regulations, that is you can configure all three types of cookie banners, or you can configure any one of the three types for your domain.

1) California Consumer Privacy Act (CCPA) - This regulation applies to the state of California (USA). To know more about the see CCPA, see CCPA FAQs.

2) General Data Protection Regulation (GDPR) - Applicable to European Union. To know more about GDPR, see GDPR FAQs.

3) Global - Applicable to the rest of the world.

- To open the Banner Configuration page, in the property selection menu, select the desired property, and then in the Cookie Consent menu, click Configure Banner.
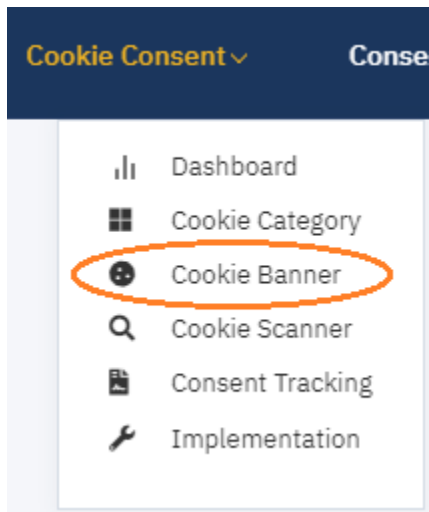
- The Banner configuration page appears.
- You can access the Cookie Scanner, Cookie Category, and Implementation page in addition to the Banner Configuration, by clicking on the corresponding tabs provided at the top left of the Cookie Banner page.
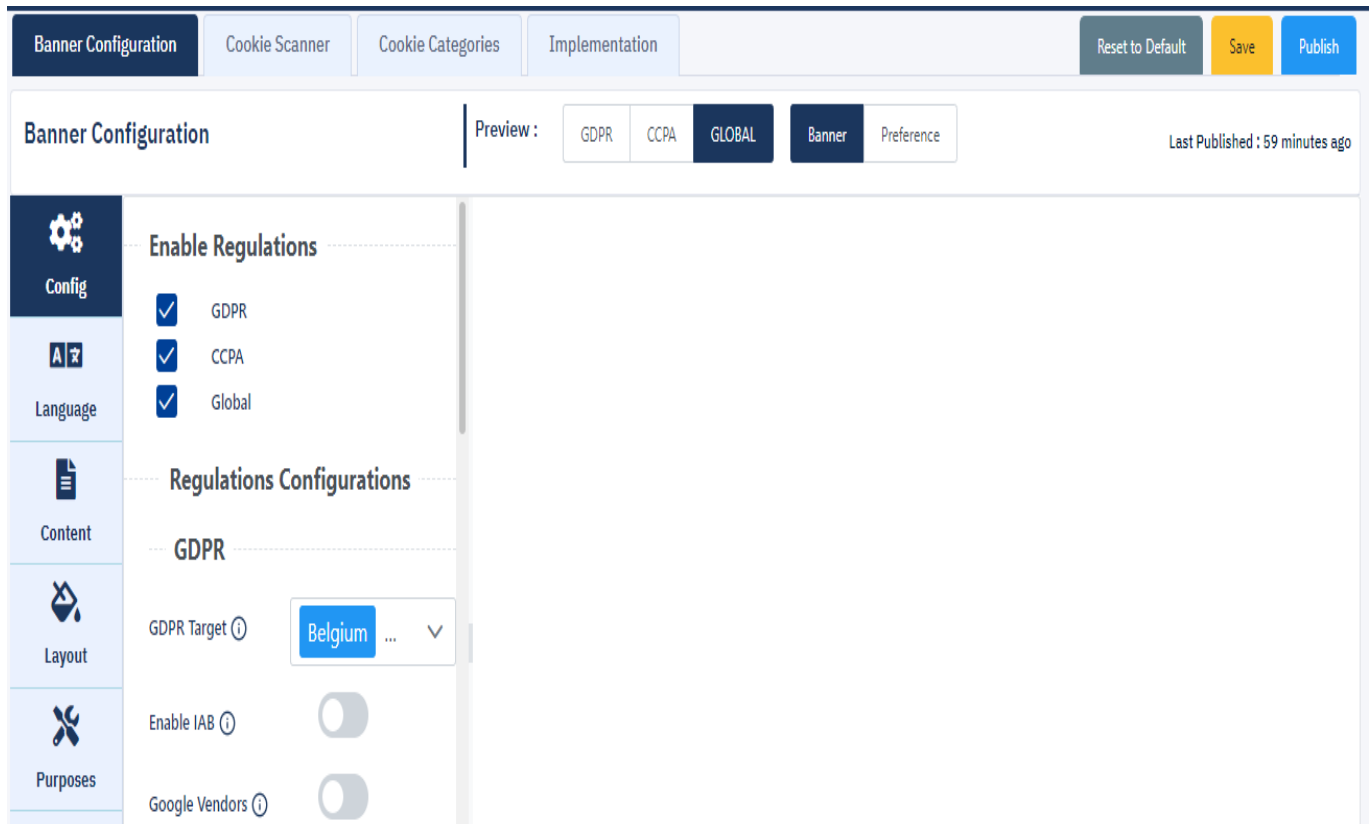
- Click the Cookie Scanner tab to get to the Cookie Scanner page.
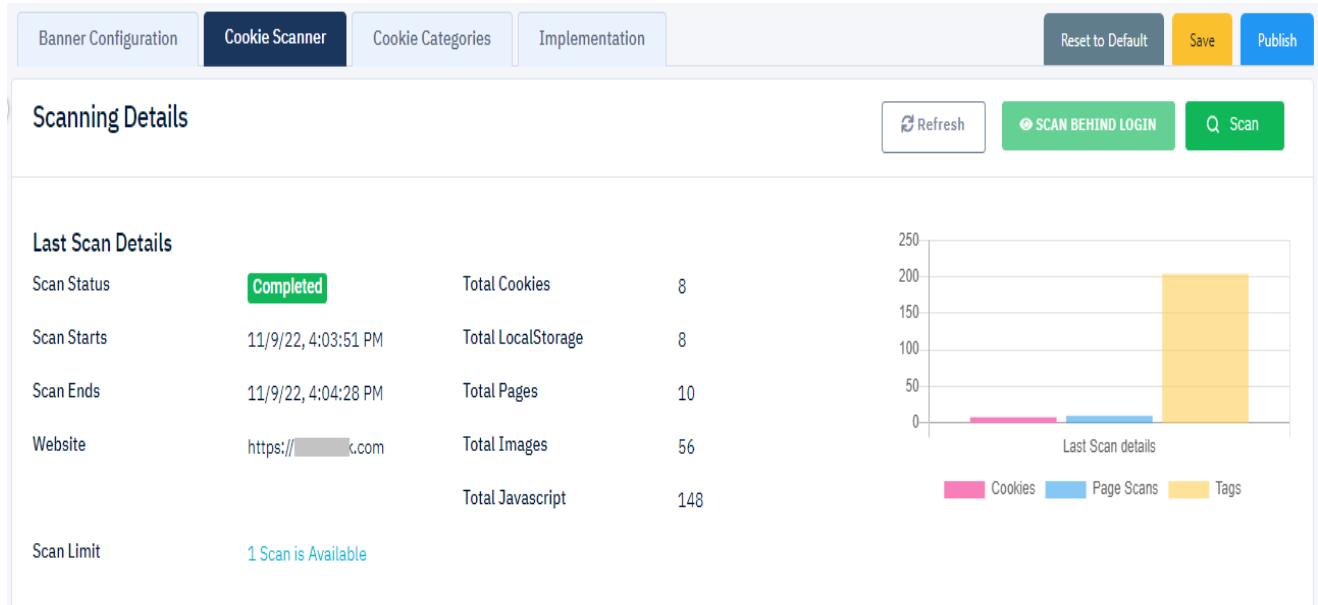
- Click the link Access the Cookie Scanner to know how to access Cookie Scanner.
- Click the Cookie Category tab to get to the Cookie Category page.
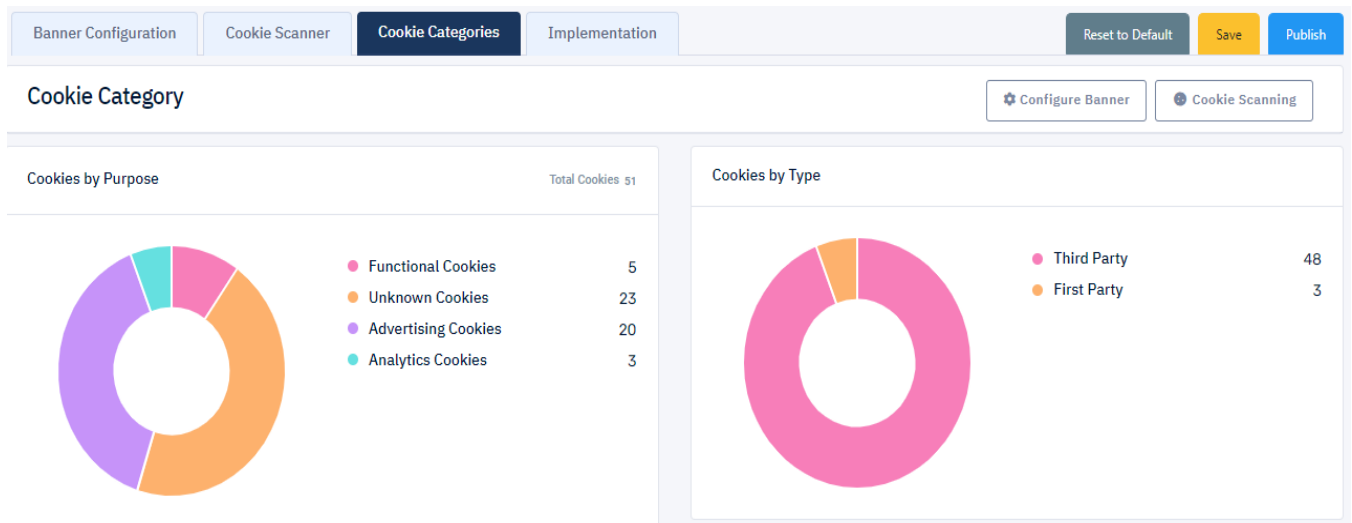
- Click the link Access to Cookie Category to know how to access Cookie Category.
- Click the Implementation tab to get to the Implementation page.

- To implement the Adzapier Application on your website click on the respective link
- [Implement on your Website HTML](#)
- [Implement on WordPress](#)
- [Implement on Shopify](#)
- [Implement on Squarespace](#)
- [Implement on Blogger](#)
- [Implement on Big Commerce](#)

Under Enable Regulations the CCPA, GDPR, and Global check boxes are kept selected by default which means you can configure cookie banners of all three types displaying on the domain.

If you don't want to configure any regulation, clear the respective check box.

Update: We have launched the cookie banner - V2. To upgrade the cookie banner on your website, publish it with the new CDN script.

Multiple Device Live Preview

You can preview cookie notices and privacy settings pop-ups of each type, while you are configuring the banner.

You can change the device at the bottom.

We Care About Your Privacy ✕

By clicking "Accept All" you provide consent to us and all the third parties mentioned in our Privacy and Cookies Preference Setting to store cookies and other technologies to enhance your website experience, process your personal data, show you personalized content and advertisements, analyze website efficiency, and improve our marketing efforts. Privacy

Privacy Settings

Disable All

Accept All

👁 Preview Device   🖥 ▢ 📱

Regulation Configurations

CCPA Banner Configuration

Follow the steps if you are configuring a banner for CCPA regulation.

1. On the Banner Configuration page, under Enable Regulations, select the CCPA check box.
2. In the CCPA Target box, select your target area, that is select California or USA.
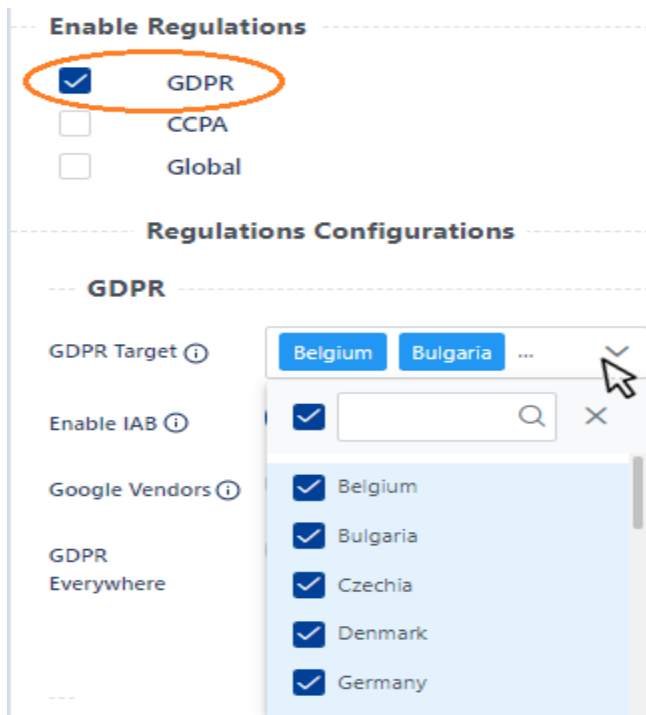
3. CCPA Target means the domain users from the selected region will get the CCPA banner and the rest of the users will get the default banner that you selected under the Advanced Features.

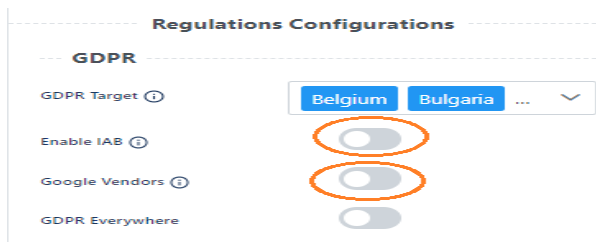4. If you want to display only the CCPA banner throughout the world, select CCPA Everywhere.
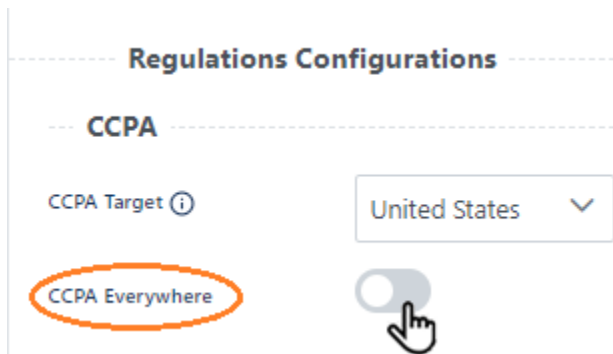
GDPR Banner Configuration

Follow the steps if you are configuring a banner for GDPR.

1. Under Enable Regulations, select the GDPR check box.

2. In the GDPR Target list, the 27 European Union countries are included by default. To remove any country from the list, clear the check box of that country. Or type the *country_name* to search and then clear.

3. GDPR Target means the domain users from the selected countries will get the GDPR banner and the rest of the users will get the default banner that you selected under the Advanced Features.

4. To enable IAB vendors and Google vendors, toggle on Enable IAB and Google Vendors respectively.

5. If you want to display only the GDPR banner, select GDPR Everywhere.

Global Banner Configuration

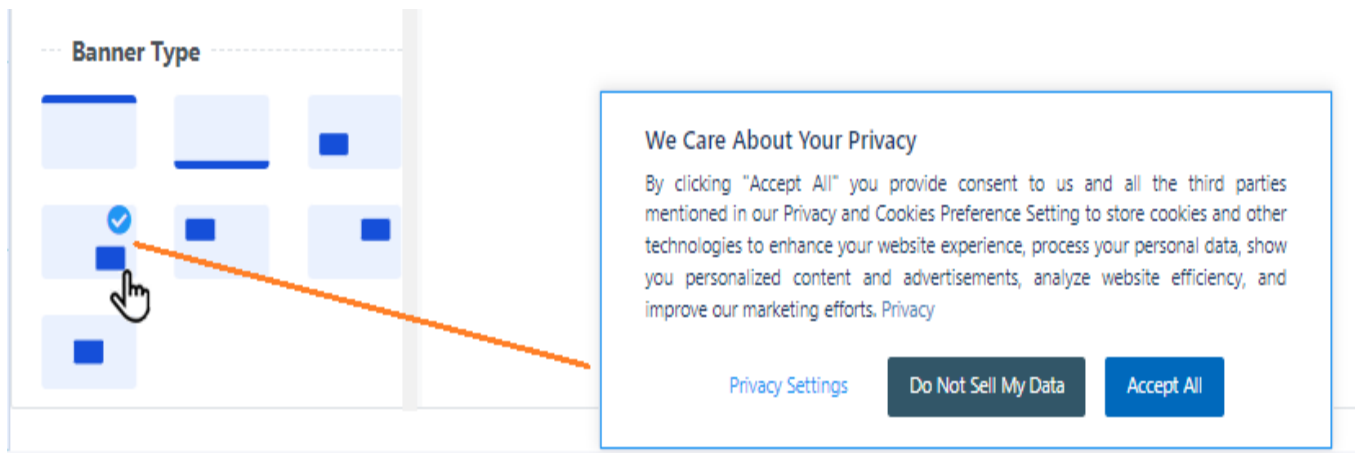To configure a global banner, under Enable Regulations, click the Global check box.

If you want to display only the Global banner, select Global Everywhere.

Banner Type

We provide two types of banners, 1) Header/footer type banners and 2) Box type banners with various positions. You can choose your appropriate type.

- Under banner type, select any banner type.

Advanced Features

Once Regulation Configuration is done, you can customize the banner using the advanced features.
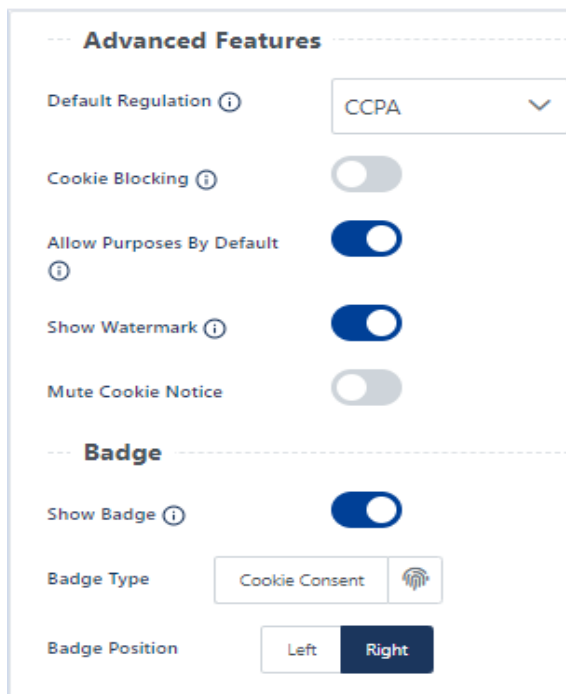
Default Regulation

- In Default Regulation, select a regulation. When users from out of the targeted area visit your domain, the selected banner type will be displayed.

Cookie Blocking

- To enable cookie blocking, toggle on Cookie Blocking and select Manual or Auto.


- To learn about this feature, see *Cookie Blocking*.

Allow Purpose by Default

- It enables allowing all the six cookie categories Essential, Advertising, Functional, social media, Analytics, and Unknown cookies by default when the domain user accepts through the cookie consent banner. To turn off allowing those cookie categories except Essential Cookies, click the toggle button.
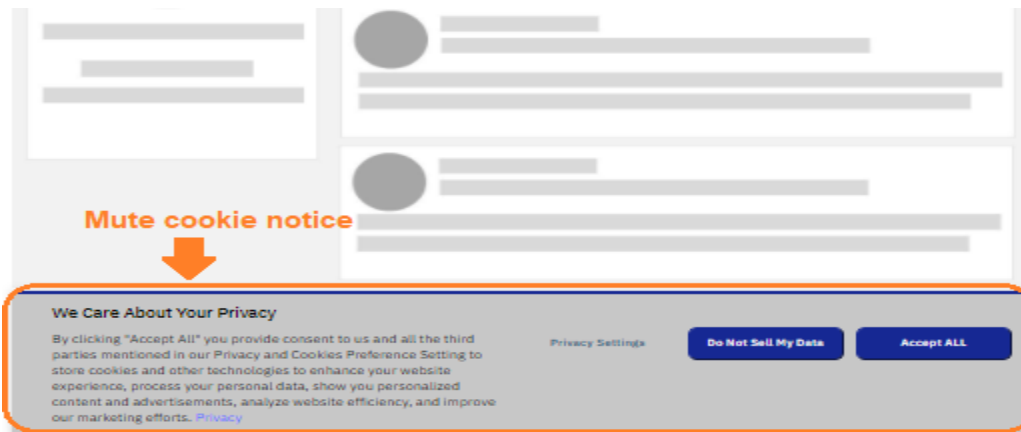
Show Watermark

- It shows the Adzapier branding watermark on the right-bottom of the privacy settings pop-up.
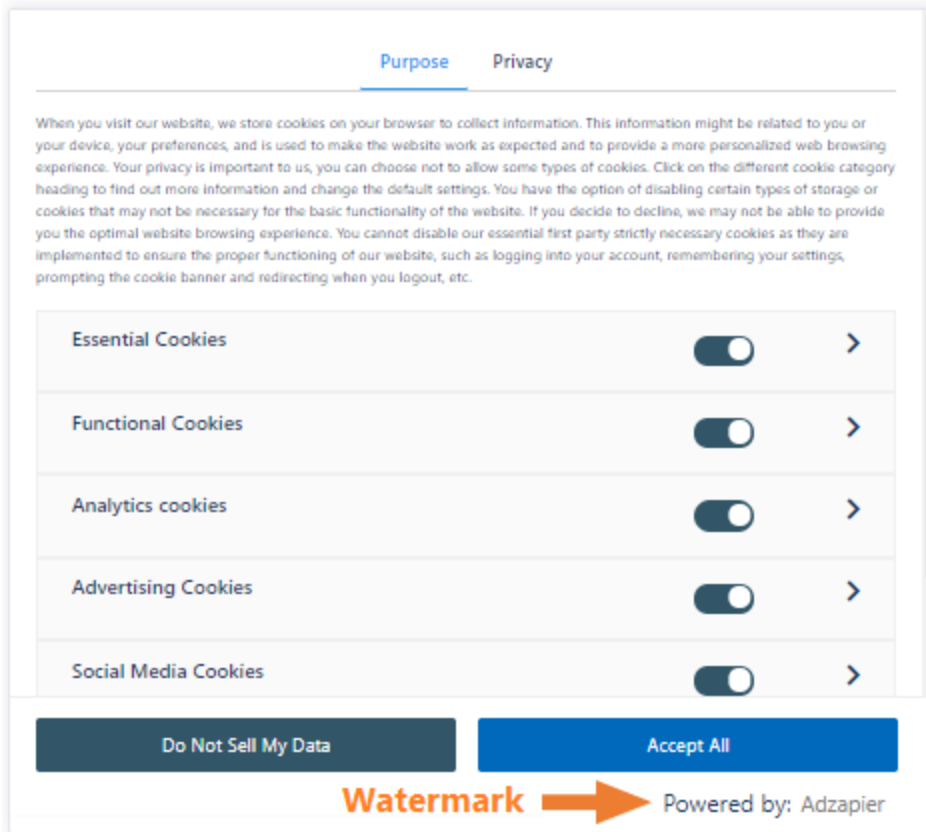
- To clear the Show Watermark, click the toggle button.

Mute Cookie Notice

- If you want to mute the cookie notice on the domain, toggle on Mute Cookie Notice.
If you enable this feature when the user visits the domain, the cookie notice will not be displayed.

Badge

- You can display a Cookie Consent badge or fingerprint icon as the badge on the domain after closing the cookie notice. When the user clicks the badge the privacy settings will pop up.
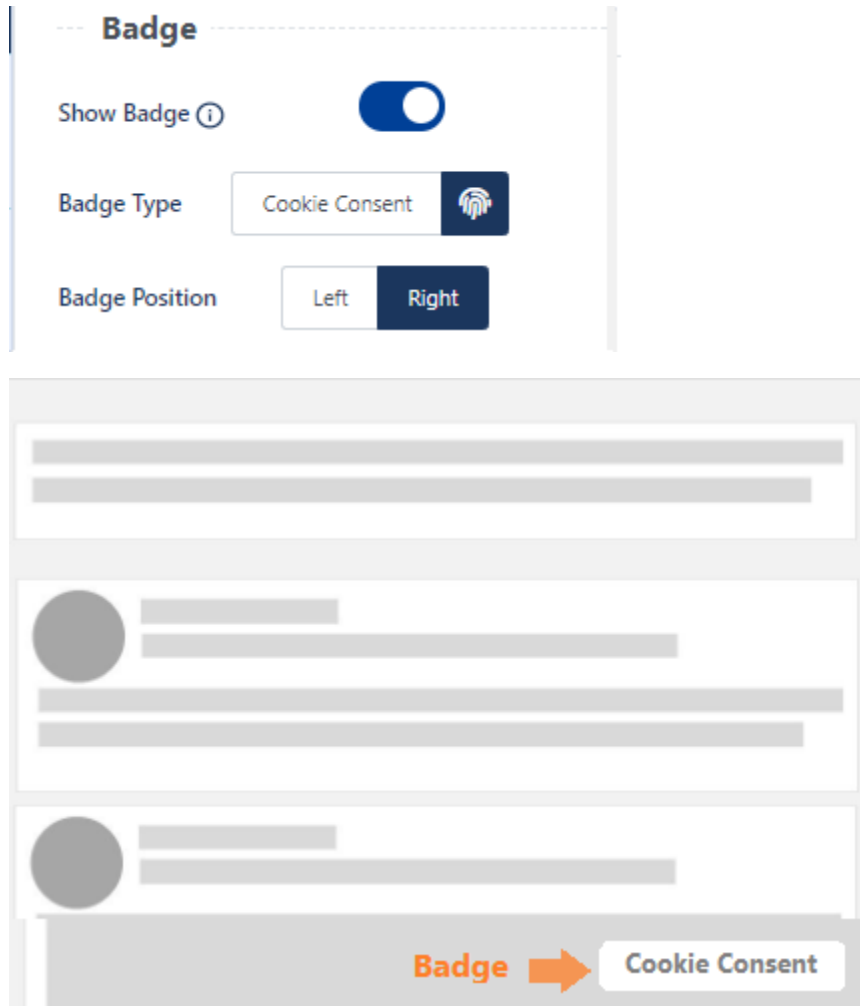
- To remove the badge, clear the Show Badge check box.

Branding

On the cookie consent privacy settings pop-up, you can add your logo.

- Under Branding, click Choose File, then upload your logo from your computer. The image of a logo in JPG, JPEG, PNG, and SVG can be supported.

- The logo preview appears below. If you want to remove the logo, click Remove below the preview.
- In the Custom CSS area, you can add CSS code to your banner to improve its aesthetic appeal. An example is given below.

Custom CSS

```
.banner-content h4{
color: blue !important;
font-size: larger !important;
font-weight: 900 !important;
}
```

- This code will turn the banner heading text color into blue, the font size will be larger, and the font-weight will be 900.

Manage Languages

You can display the consent banner in various languages like English, Chinese, French, and so on.

The default language of the cookie banner is English. But you can add more language options using settings.

1. On the Banner Configuration page, click the Languages tab.
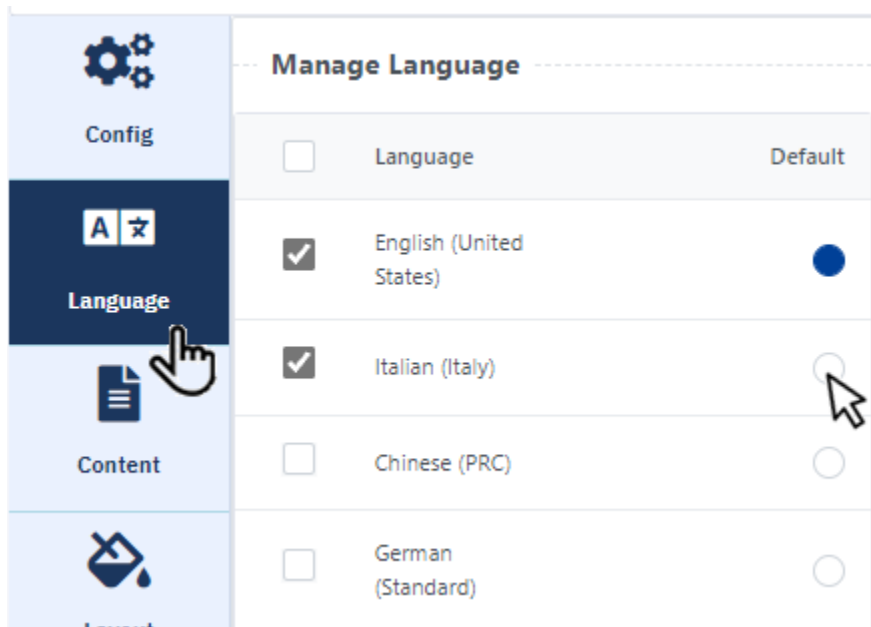
2. To add any languages from the list, click the check box right to the language. The selected language options will be added in the privacy settings.

3. To make your preferred language as default, select the language, then click the button in the Default column right to the language.

Note: The banner is displayed on your domain in the default language. The user can change the banner language with Privacy Setting.
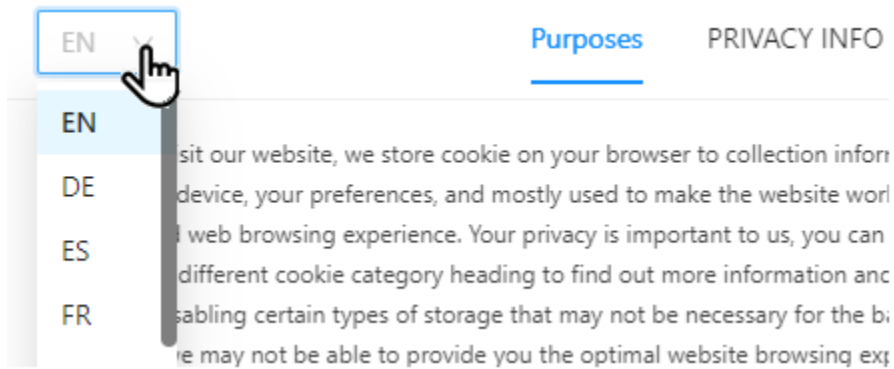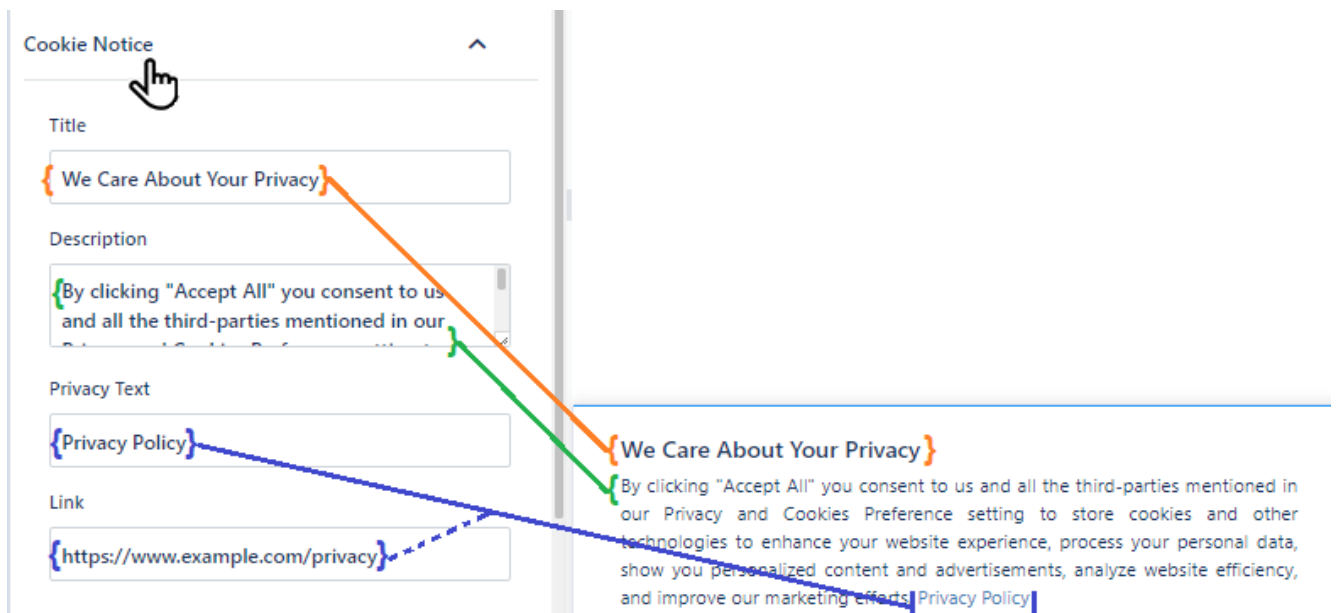

Edit Contents

Banner Content

You can edit the content of the cookie banner and the privacy policy link.

- Click the Content tab and under Banner click Cookie Notice.

- It shows the content of the GDPR banner.
- In the same way, you can edit the contents of the CCPA and Global banner also. In Live Preview, you can change the regulation.

Banner Buttons

You can edit each button title of every regulation banner.
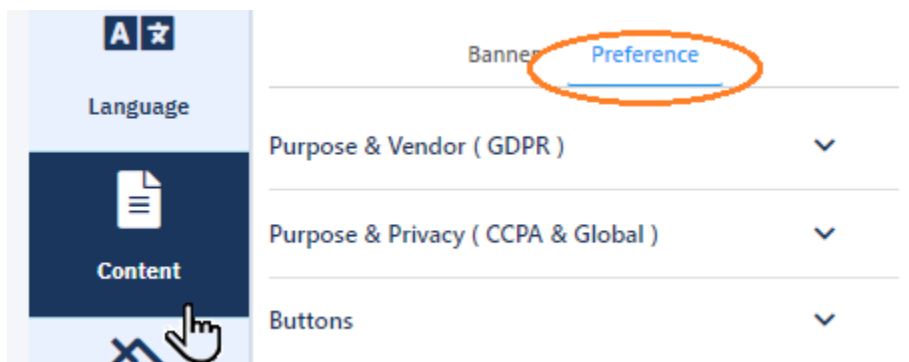
- In the Content tab, under Banner, click Buttons.

- In Live Preview, select CCPA or Global. In the same way, you can edit other button titles.

Preference (Privacy settings) Content

You can edit the contents and button names of the privacy settings pop-up.

- In the Content tab, switch to Preference.

In the privacy settings of the GDPR banner Purpose and Vendors tabs with their descriptions are available and edit the content of those descriptions. In Purpose Description, you can edit the text.


- In the same way, you can edit the Vendors Description.
- In Live Preview, select CCPA to edit Purpose and Privacy descriptions. In the same way, you can edit descriptions of the Global regulation banner.

Preference Buttons

- In the Content tab, under Preference click Buttons to edit the button names.
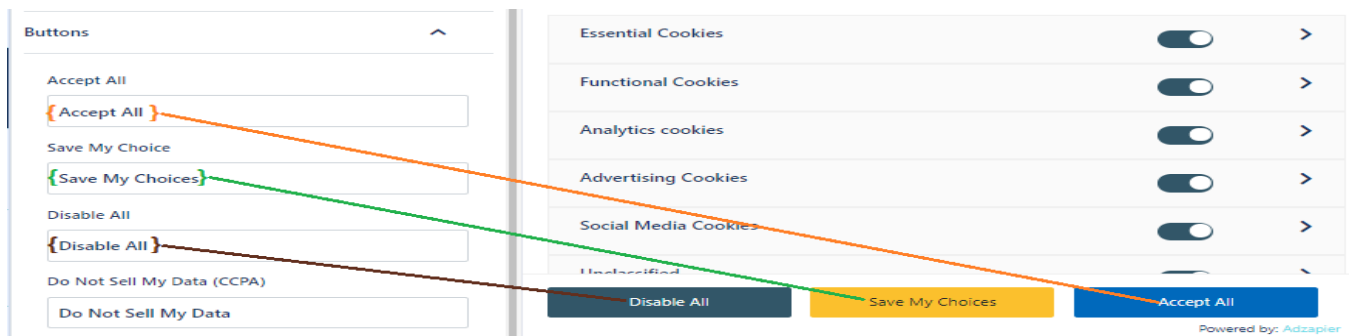
Note: If you added multiple language options, whatever you make the changes in the contents, make the same changes with every other language too. To change the preview language click Preview Language and select another language to edit.
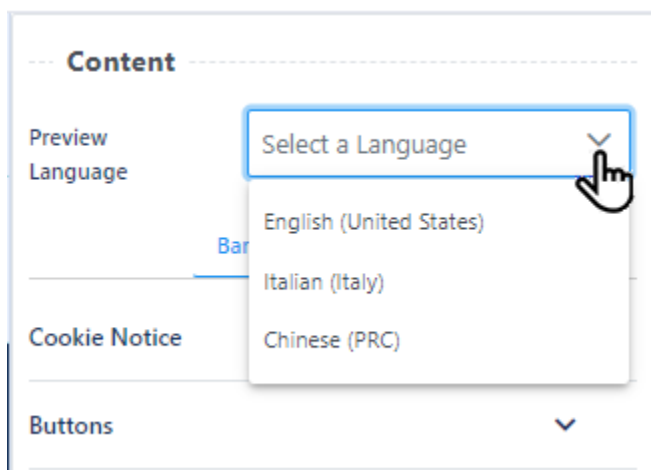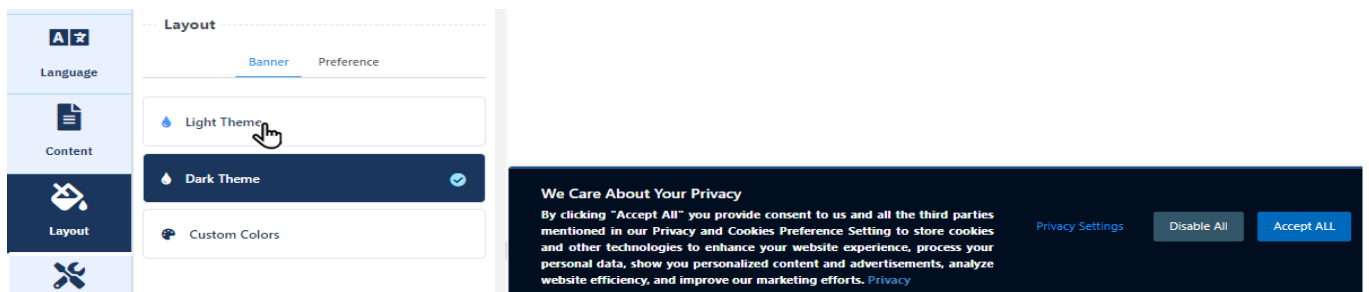

The languages you added through the Languages setting will appear here.

Layout

Banner Layout

- You can select a Light Theme or Dark Theme for the banner.

- To customize the theme, click Custom Theme, then click Cookie Notice, and you can customize the colors of the Background, banner Text, Border, and Privacy Link.

To change the color, click the color box and select a color or enter a color code.

- You can customize the name and color of each button.

- In Live Preview, select other regulation banners to customize the buttons.

- You can customize the margin of the cookie notice too.
- Click Margins and you can customize all-around margins by increasing or decreasing the pixel value.

- You can also customize the cookie notice padding.
- Click Padding, and you can customize the pixel value.

Preference (Privacy Settings) Layout

To customize the privacy settings pop-up, switch to Preference and click Custom Theme.

- To change the background and text colors, click Preference.

- To customize the colors of the cookie category, click Purpose.

- You can customize the buttons of the privacy settings pop-up. Click the Accept All tab.

- In the same way, you can customize the other buttons. For the other regulation banners, in Live Preview, select the other regulations to customize their buttons.

Badge Layout

- You can customize the cookie consent badge colors too.

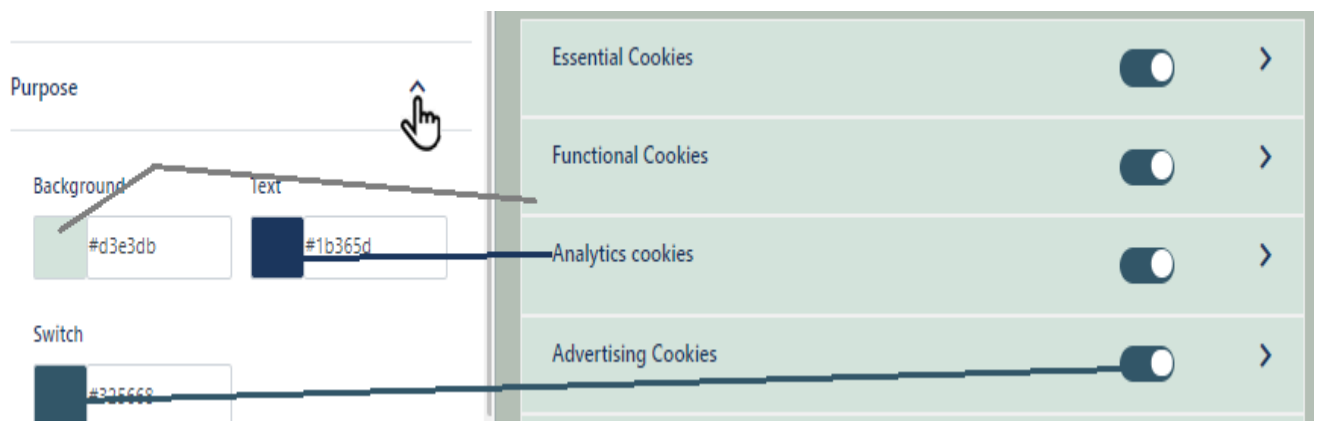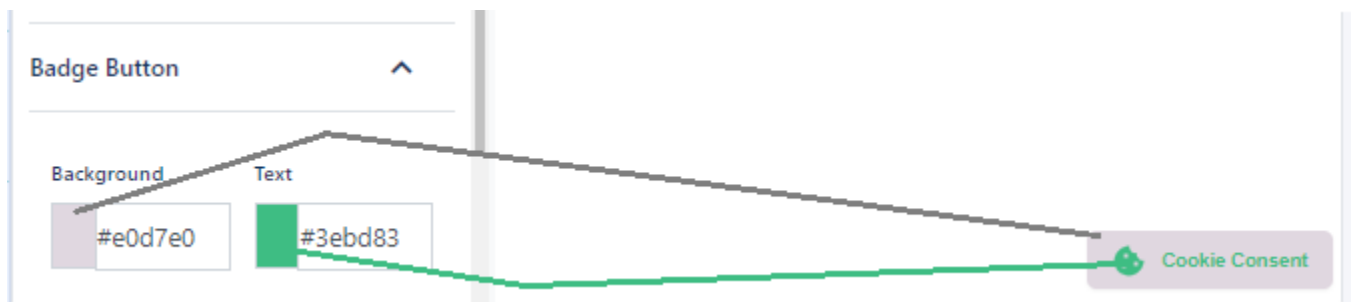- Click Badge Button and customize the colors.

Manage Purposes

In Manage Purposes there are six cookie categories with their respective descriptions available which are customizable.

- There are six categories by default, you can deselect any category which is not applicable to your website. To be more precise, as per the cookie scan results, you select which cookies are present and unselect the others.
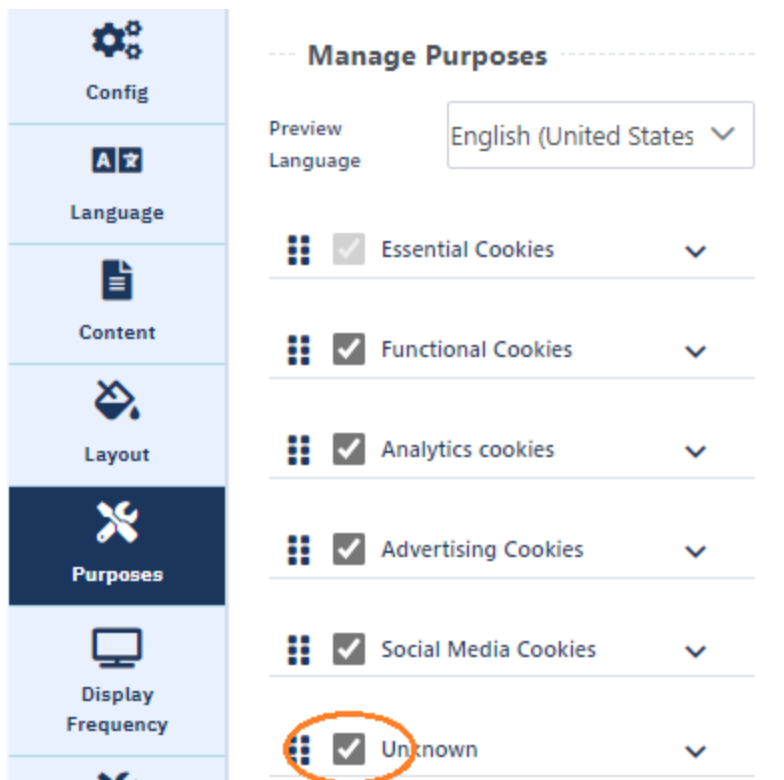
- To reposition any cookie category tab, click ⠿ and drag to the desired position.
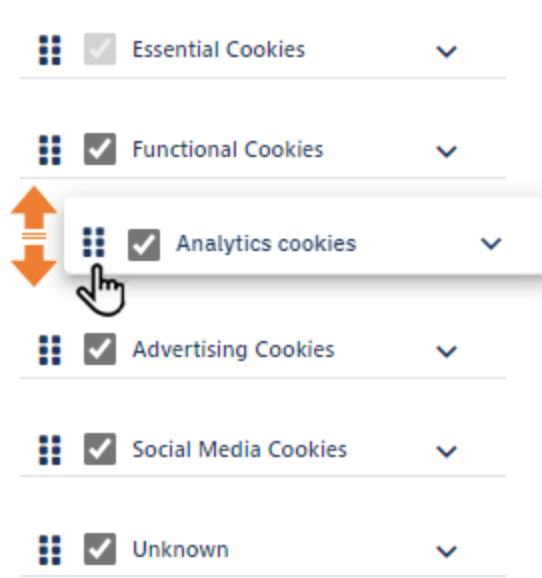
- To edit the title and description of any cookie category, click the category and click the same category in the preview. Now you can edit the category title and description.
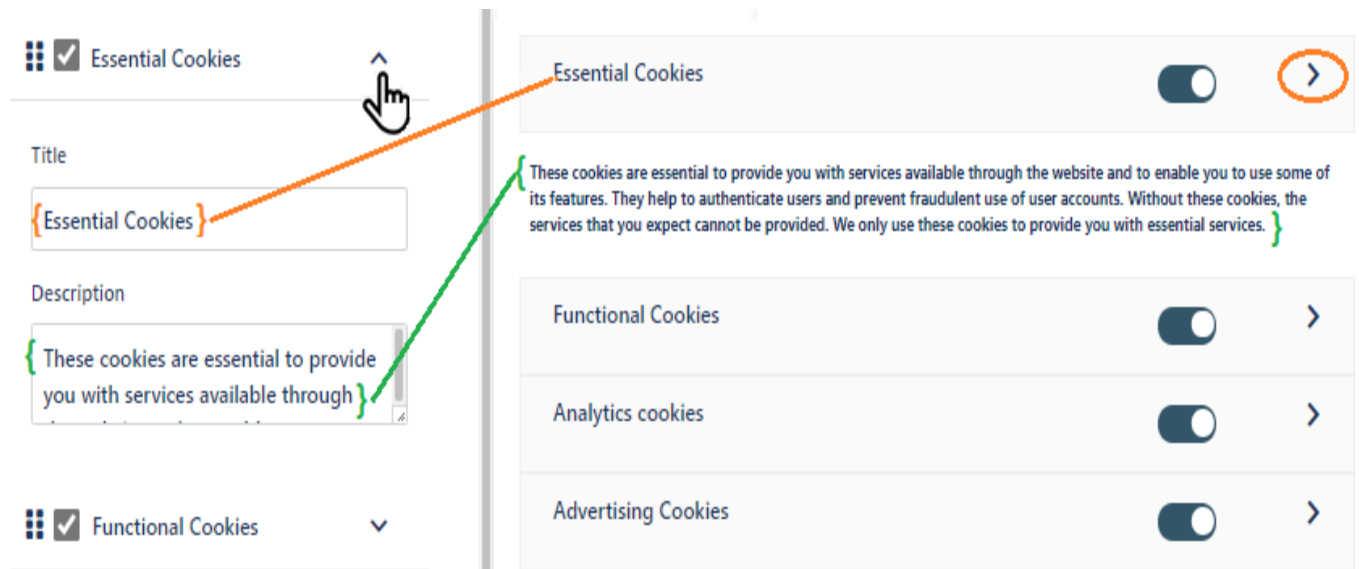
Display Frequency

If you want to define the frequency of displaying the banner, which means the repetition of cookie banner display for the various actions from the website user.
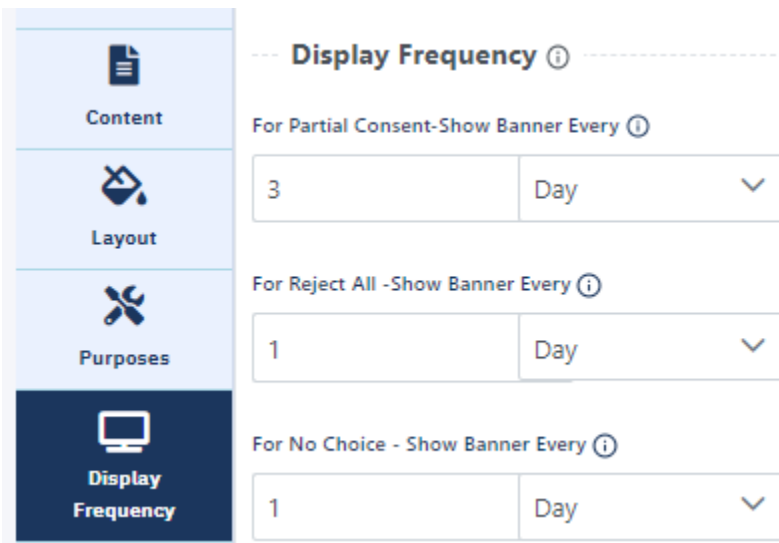
1. Enable Display Frequency.

2. Hover over ⓘ to see the description of each setting.

3. To change the frequency of displaying the cookie banner, enter a value or click ∧ or ∨ to change the value.

4. Select any span Hour, Day, or Page View.
   Page View means the cookie banner displays after a specific number of visiting the domain.

Manage Vendors

1. For the GDPR, if you enable IAB and/or Google vendors, you manage the list of vendors under the Manage Vendors tab.
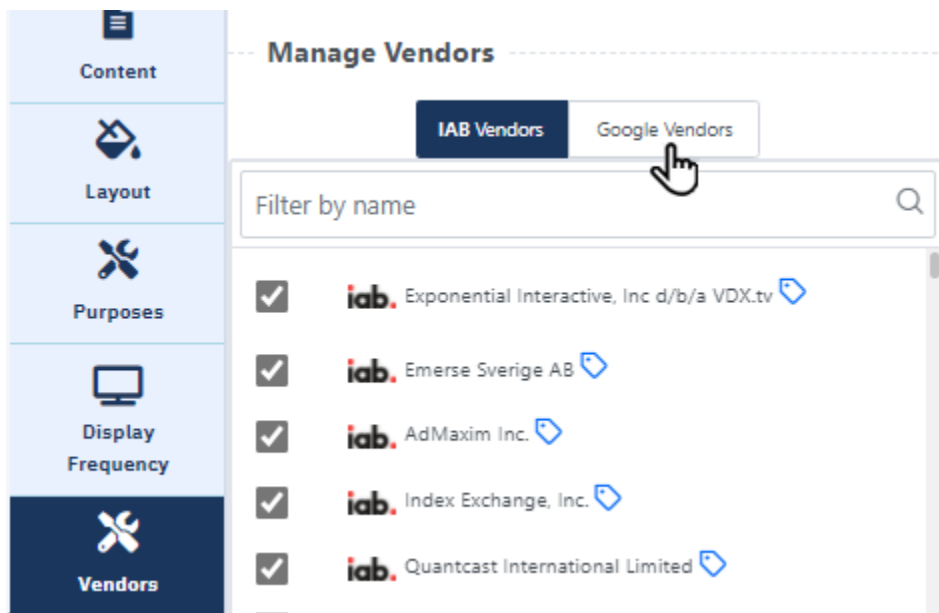
1. It shows IAB vendors by default. To view the Google vendors, click Google Vendors. By default, all vendors are active.

2. To deactivate any vendor, clear the check box. In the search box type a *vendor's name* to search.

3. To see the privacy policy of any vendor, click ⬦ right to the vendor's name.

4. You can allow all the vendors by clicking on Allow All and disallow all by clicking on Disallow All. By default, all the vendors are allowed.
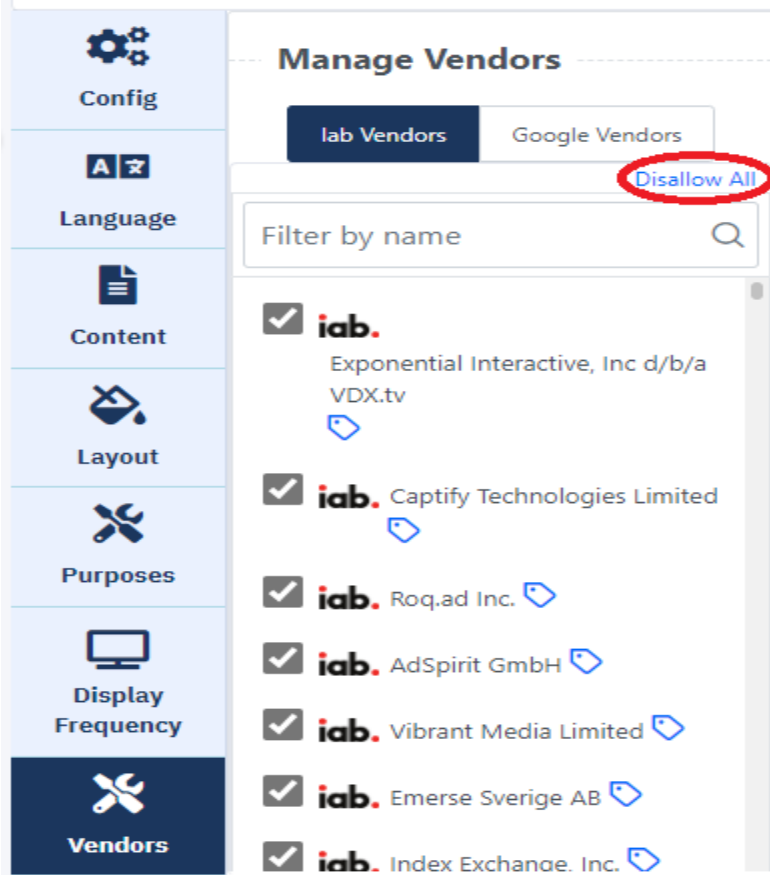
Save and Publish

1. To save the progress of your configuration, click Save.
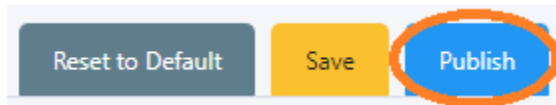
2. Once you have completed all the configurations, click Publish to implement the banner on your website.
   A Production CDN script pop-up will appear.

Production CDN

Copy Script

```
//Please copy and paste this code into the header for each page on
   your website(s). It is important that this code be the first
                    script in your document.
  <script type="application/javascript" src="https://staging-
      cdn.adzapsrv.com/cmp/v2/web/b557ede6-7e48-42d7-af33-
  64ad7b0d264e/8323d855-4c24-4e28-a0f3-17c1cc64a0eb-bundle.js">
                            </script>
```

How to integrate Adzapier scripts to:

Go to Dashboard   Implementation

3. On the other hand, you can proceed to the Implementation page by clicking the Implementation button or the Implementation option in the cookie consent menu.

4. Click Copy Script, the script is copied to the clipboard. Now you can add this JS code to your website code to publish the banner.

   Note: On the webpage of your domain where you want to implement the Cookie Banner, you must insert the CDN script before the </head> closing tag.

5. If you want to learn how to integrate the Adzapier script into your website, click on the respective site and follow the steps.

How to integrate Adzapier scripts to:

Go to Dashboard   Implementation

Note: If you want to reset the configuration to the default, click Reset to Default and click I Agree.

Update Cookie Banner

To make any changes to your cookie banner,

1. Go to the Cookie Banner configuration page, make any changes, then click Save.
2. When you click Publish, it asks for confirmation to let your website users give consent again.
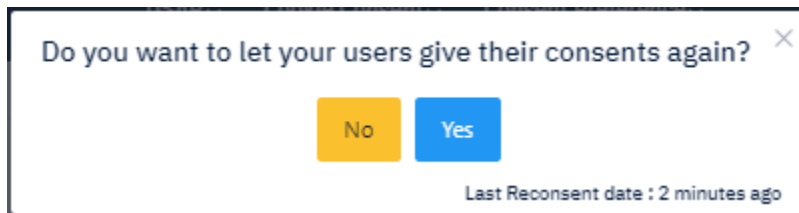
1. If you click Yes when the users visit your website or refresh the page, the cookie notice will appear again. Or else click No.

   Note: After making any changes to the cookie banner and you must publish it again to reflect the changes on your domain. Once you published, it may take several minutes to reflect on your production.

Publish History

You can see the cookie banner's version history, as well as manage them.

- At the bottom-right of the page, click Publish History.

- The publishing history appears.
- If you have a sequence of versions, you can roll back into an older version or you can delete the version.

- Click ⋮ and click Rollback or Delete.

Consent Tracking

With your Adzapier portal account, after successfully publishing your banner to a property, you can track the details of the cookie consent which had given by the users of the domain.

Individual Consent Details

1. In the property selection menu, select the desired property.

2. In the Cookie Consent menu, click Consent Tracking.
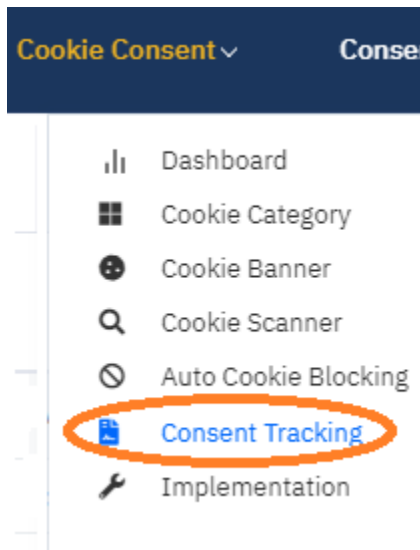
The Cookie Consent Tracking page appears.

3. Select any date range.
   A list of the cookie consent appears.

> Tip: It shows all cookie consent details within your selected date range. To flip the page, click > or <, and to set the number of items to be viewed per page, click ˅ and select a number.

Apply Filters to Sort out.

To apply the filters, click

The filter pop-up appears.

- Filter by Banner Type - click the Select Consent Type box and select any consent type and click Apply.
  The list will be sorted out accordingly.
- Filter by Status - You can sort out the list by the Status of the consent.
- Filter by Country - You can filter the list by Country.

You can also sort by Type, Status, Date, and Country and view the result.

View Details of a Particular Cookie Consent

To view the details of a particular cookie consent, click the ID of the cookie consent.

A separate Consent Details page appears for each cookie consent.

On the Consent Details page, several details are available.

If the user of the domain had given consent through the Generic type cookie banner, it shows the following details.

- Consent Information panel contains various details such as date of consent, banner type, location, and user's system information.
- Generic Consent string (1- - -)
- A checklist of the Allowed Cookies.

Allowed Cookie Consents	
Essential	✔
Functional	✔
Advertising	✘
Social Media	✘
Analytics	✔
Unknown & Unclassified	✘

- In the above example, the user had allowed Essential, Functional, and Analytics Cookies and disabled the Advertising, Social Media, and Unknown & Unclassified cookies.

If the user had given consent through the CCPA-type banner, the following details are shown.

- Consent Information panel
- US Privacy String (1YYY or 1YNY - the description of the string is available on the Consent Details page)
- A checklist of the Allowed Cookies.

If the user had given consent through the GDPR-type banner, the following details are shown.

- Consent Information panel
- IAB Decode Information
- A checklist of the following

  - Purpose Consents List

  - Allowed Cookie Categories

  - Vendors List

  - Special Purposes List

  - Features List

  - Purpose Legitimate Interest

- Vendor's Legitimate Interest
- Special Feature Options
- Google Vendors

Cookie Blocking
What are Third-Party Cookies?

Third-party cookies are the cookies set by websites that are outside of your current domain. They are mostly used to track users between websites and display more relevant ads on the domain.
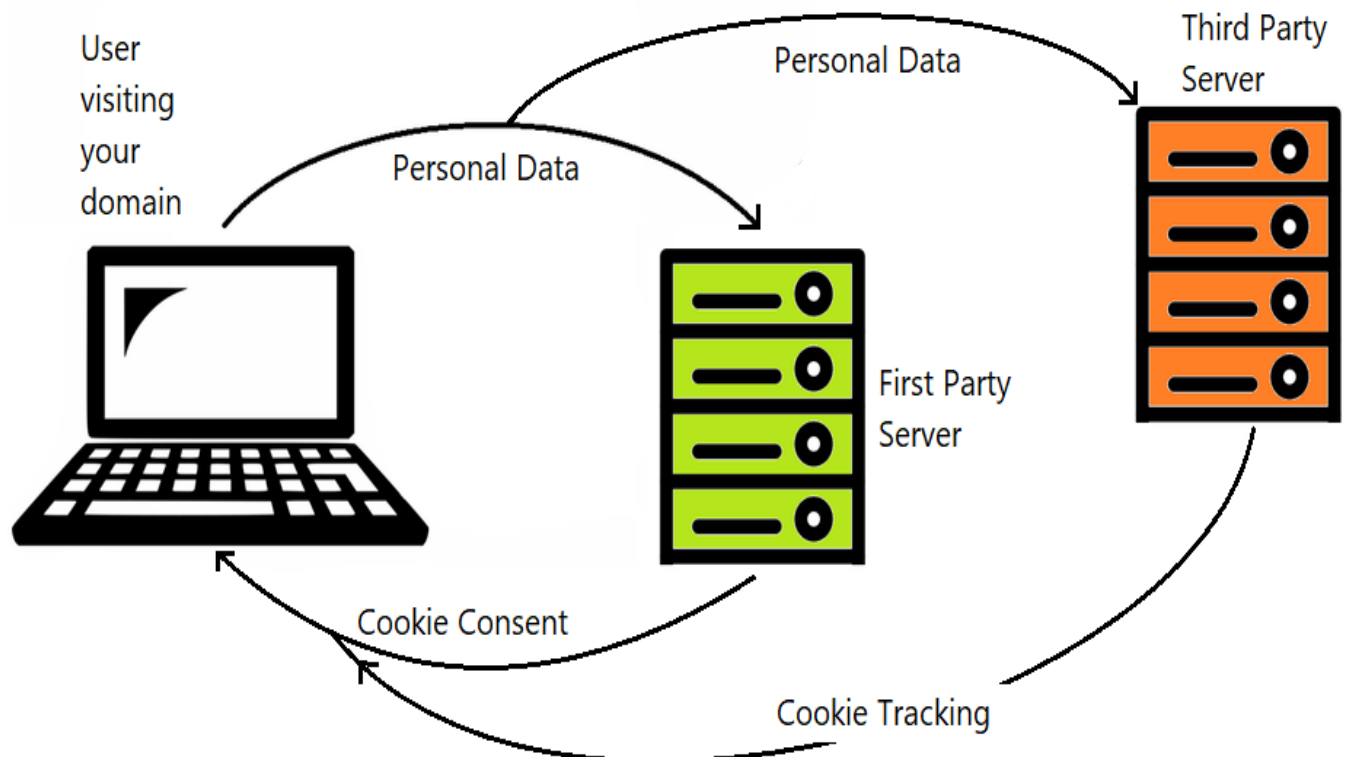
For example, the cookies used by Facebook like-button on your domain, support chat functionality provided by a third-party service, and so on. Another example is an advertising service (ex: Google Ads) which also creates a third-party cookie to monitor which websites were visited by each user. This is the main technology used to show you the product ads that you previously searched for on a completely different website.

Why Do You Need Cookie Blocking

If you want your domain to comply with the latest regulations such as CCPA and GDPR, you might want to block those third-party cookies unless the user specifically agreed to use them. This article explains how to establish cookie blocking using Cookie-Script as a cookie compliance solution.

Automatic Cookie Blocking

Adzapier provides Automatic Cookie Blocking, a special feature to block cookies at your website user side until the user gives consent through Adzapier's cookie banner. With this feature, you can block the cookies of any category except strictly necessary cookies and when the user allows any categories through the cookie banner, the set cookies under those categories will be enabled.

How Auto Cookie Blocking Works

- The list of hosts is getting from cookie scan results and the same will be displayed on the Auto Cookie Blocking configuration.
- When you enable Auto Cookie Blocking you can select and categorize third-party hosts that you want to block.
- When any categories (other than Strictly Necessary) have not been consented by the website user, the scripts of the hosts under those categories will not be loaded on the website.
- When the website user consents to those categories, then the scripts of the hosts will be loaded.

Implement Auto Cookie Blocking

When you configure the cookie banner, you can configure the automatic cookie blocking as follows.

1. In Banner Configuration, under Advanced Features, enable Cookie Blocking.

2. Select Auto and save your configuration.
3. Now, in the Cookie Consent menu, click Auto Cookie Blocking.
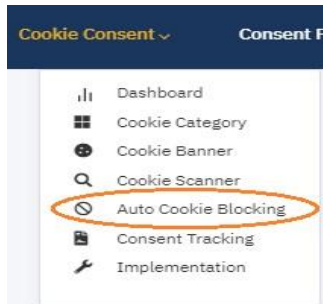
- The Auto Cookie Blocking page will appear. On the Page's upper right corner, you can notice an Add Scripts Button. Click on the Button.
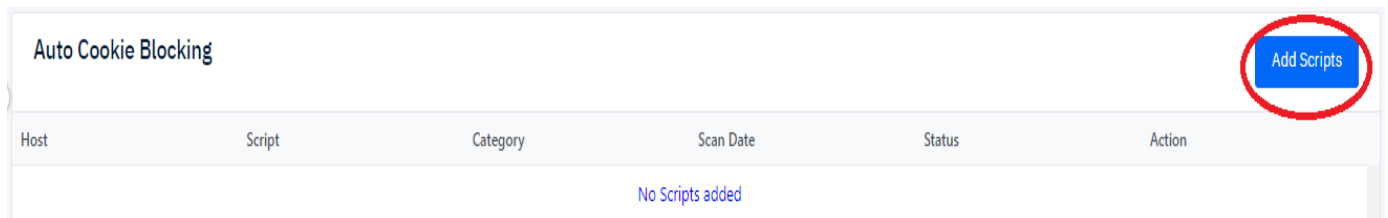
4. A list of hosts appears from the cookie scan results.

Add Script
×

Host	Script	Category	Scan Date	Status	Add
cdn.primeconsent.cc	https://cdn.prime consent.com/cm p/consent- preference/prod uction/adzapier- cp-sdk.js	Please Select the Category	Sep 5, 2022	DISABLED	⊕
adzapier.com	https://adzapier. com/wp- content/plugins/ elementor/assets /js/webpack.runti me.min.js? ver=3.7.3	Please Select the Category	Sep 5, 2022	DISABLED	⊕
cdn.primeconsent.cc	//cdn.primecons ent.com/cmp/v2/ web/39d8face- ec86-49a0-a3d7- 39170528ec18/fa 1903a4-ebd0- 43bb-b772- 7f4c3242e292-	Please Select the Category	Sep 5, 2022	DISABLED	⊕

5. You can add as many hosts by clicking the ⊕ icon.

- By default, the status of all hosts shows DISABLED, which means cookie blocking is disabled, and these hosts will appear on the website on the user side.

Click ✎ right to the host that you want to block.

| resources.blogblog. | https://resources.blo | -- Disable... ⌄ | | DISABLED | ✓ ✕ |

6. In the Cat___ry dropdown, select an appropriate category for the selected host, and click ✓ .

- The cookies associated with this host gets blocked on the website-user side until the user gives consent to the specified category.

7. After completing the configuration, go to the Banner Configuration and proceed further.

Note: After publishing the cookie banner, whenever you make any changes in Auto Cookie Blocking, you must publish the banner again to reflect the changes.

Manual Cookie Blocking

You can block third-party cookies by blocking the whole third-party functionality. This means Google Analytics, Facebook buttons, AdSense, and anything else that you block won't work until the user agrees with cookie consent. You can manually achieve this in the following ways.

Blocking Third-Party Cookies Set with JavaScript

To block third-party cookies, find a JavaScript code that is setting third-party cookies and follow the steps.

- Change `type` attribute from `text/javascript` to `text/plain` (if `type` attribute missing, just add it)
- If you have scanned your website for cookies, add `az-data-cookiecategory` attribute. Below is a list of available values for this attribute. If you don't have cookie category choices, you can skip adding this attribute.

Blocking Third-Party Script by Cookie Category

If all the cookies from a third-party script are assigned to a certain category, you should include that category in `az-data-cookiecategory` attribute of the script.

The `az-data-cookiecategory` attribute should have a value of the cookie category that this third-party JavaScript is assigned to. This means that whole third-party service

cookies should be assigned to one of the following categories (which is usually the case). Possible category values are:

- Necessary cookies: `necessary`
- Functional cookies: `functional`
- Advertising cookies: `advertising`
- Analytics cookies: `analytics`
- Social media cookies: `socialmedia`
- Unclassified & Unknown cookies: `unknown`

All JavaScript with such attribute changes will only execute if the user agreed with Cookie Policy.

Note: It is possible to assign third-party scripts to the above categories, this is helpful if the third-party script sets cookies from the categories and the user must agree to all cookie categories that are set by the script.

To use multiple categories, list them all separated by a space. In this case, a third-party script will be included if the user agrees to all categories listed in the `az-data-cookiecategory` attribute:

```
<script type="text/plain" az-data-cookiecategory="funtional">
```

Example of Included JavaScript File

Change code from:

```
<script src="/js/myscript.js"></script>
```

Change code to:`<script type="text/plain" az-data-cookiecategory="functional" az-data-src="/js/myscript.js"></script>`

Blocking Third-Party Cookies Set with an iframe

To block third-party cookies set with iframe (like YouTube videos), find an iframe code that is setting third-party cookies and follow the steps.

- Change `src` attribute name to `az-data-src`.

- If you have scanned your website for cookies and have category checkboxes in the cookie consent pop-up, add `az-data-cookiecategory` attribute. Use the same list of categories as described in the previous section of this article. If you don't have cookie category choices, you can skip adding this attribute.

All iframes with such attribute changes will only show up if the user agreed with Cookie Policy.

Change code from:

```
<iframe  height="350" src="https://www.youtube.com/embed/xxxxxxxxx" frameborder="0" allowfullscreen></iframe>
```

Change code to:

```
<iframe  height="350" az-data-src="https://www.youtube.com/embed/xxxxxxxxx" alt="Please accept cookie policy first" az-data-category="functional" frameborder="0" allowfullscreen></iframe>
```

Blocking Images of third-party cookies

In the same manner, you can block image/object elements from setting third-party cookies.

Example of Image Element

Change code from:

```
<img src="http://example.com/image.jpg"/>
```

Change code to:

```
<img az-data-src="https://picsum.photos/200/300/?blur" az-data-category="functional"/>
```

Scan Behind Login
Why do you need Scan Behind Login?

When your website has an authentication form that allows the users to log in with their credentials, the regular cookie scanning feature doesn't able to detect the authentication cookies like sign-up or sign-in forms, and other cookies associated with your account.

In such a case, you can use our special cookie scanning feature named Scan Behind Login to detect all cookies even behind the login.

When you are subscribed to an Enterprise plan of Cookie Consent Management for your website property, you can get Scan Behind Login feature on the Cookie Scan page.
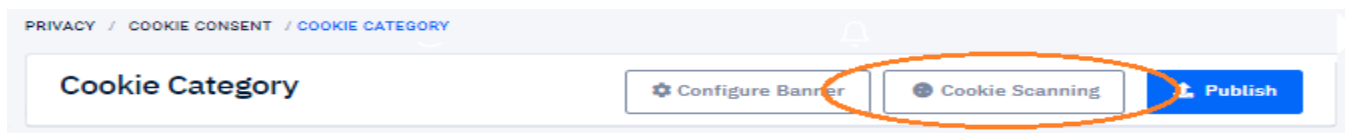
Prerequisites: Login credentials

The following is the procedure to perform a scan behind login.

1. In the menu, select the property.

2. Select the property that you want to scan.

3. In the Cookie Consent menu, click Cookie Category.
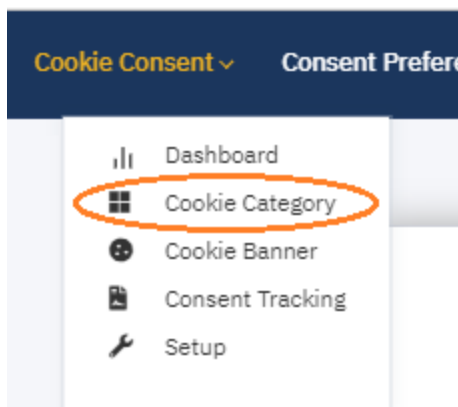
The Cookie Category page appears.

4. Click Cookie Scanning.
   The Scanning Details page appears.

Scanning Details

⟳ Refresh | ⊙ SCAN BEHIND LOGIN | ⚲ Scan

5. Click Scan Behind Login.
   The Scan Behind Login form appears.

How to Fill the Scan Behind Login Form

Follow the procedure to duly fill out each field of the form.

1. Website Login URL - Enter the login page URL.

Scan Behind Login Form   ✕

* Website Login URL ⓘ

https://www.linkedin.com/login

* Redirect URL ⓘ

https://www.linkedin.com/feed/

2. Redirect URL - Enter the webpage URL redirected after you log in successfully.

3. Username/Email Type
   >Inspect the Username/Email field of the login page. See the example below.
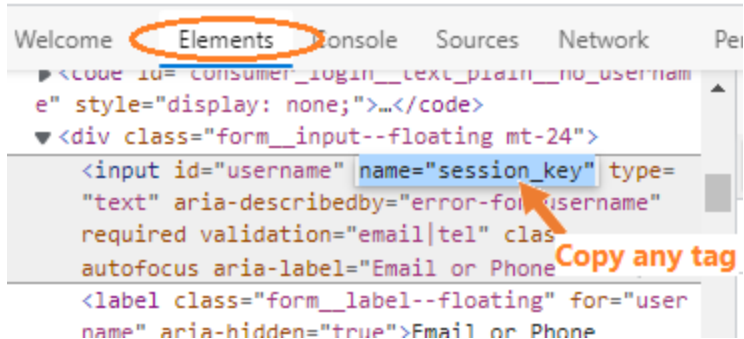
Email or Phone

Right-click > Inspect

Password   show

Forgot password?

> Right-click the Username field and click Inspect.

The development tool appears. Under the Elements tab, the corresponding field element gets highlighted.

> In the Input element, copy any tag like `name="..."`, `type="..."`.
> Now go to the scan behind login form, in the Username/Email Type field, type "input[ ]", then insert the copied tag in between the square brackets, and replace the double quotes with the single quotes. See the example below.
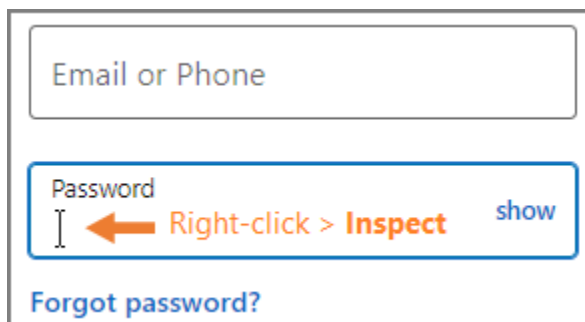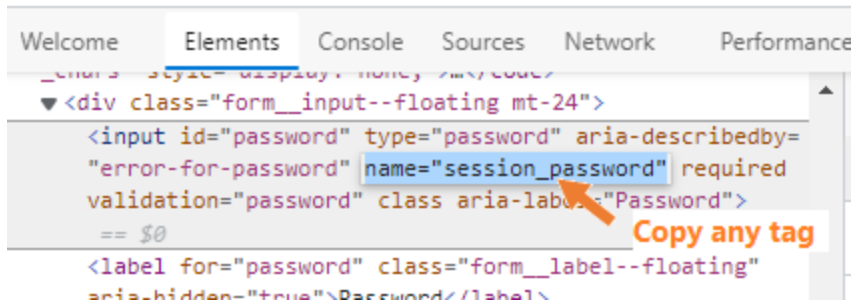

4. Username/Email - Enter the *username* or *email-id*.
5. Password Type
   > Inspect the password field of the login page. See the example below.

> In the Input element, copy any tag like `name="..."`, `type="..."`.

> Now go to the scan behind login form, in the Password Type field, type "input[ ]", then insert the copied tag in between the square brackets, and replace the double quotes with the single quotes. See the example below.
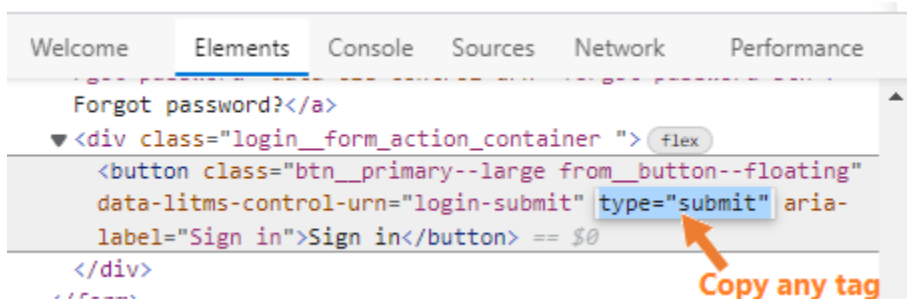
Password Type ⓘ

input[name='session_password']

6. Password - Enter the *password*.

7. Button Type
    > Inspect the Log-in/Sign-in button of the login page and get any button element tag. See the example below.

> Now go to the Scan Behind Login form, in the Button Type field, type "button[ ]", then insert the copied tag in between the square brackets, and replace the double quotes with the single quotes. See the example below.

Button Type ⓘ

button[type='submit']

Another example is given below for an input type submit function.

```
▼<div class="submit-container move-submit-down">
    <input type="submit" name="commit" value="Sign
    in" class="gl-button btn btn-confirm" data-qa-
    selector="sign_in_button" data-disable-with="Si
    gn in"> == $0
</div>
```
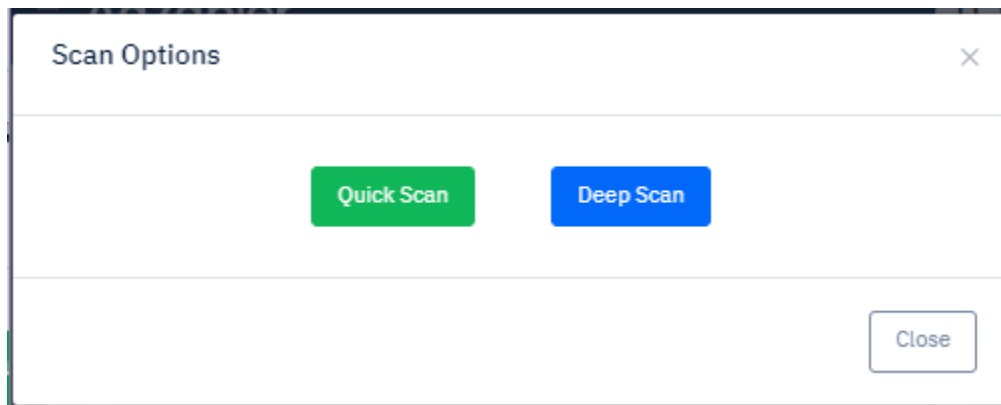
In the above case enter the Button Type in the below format

Button Type ⓘ

```
input[type='submit']
```
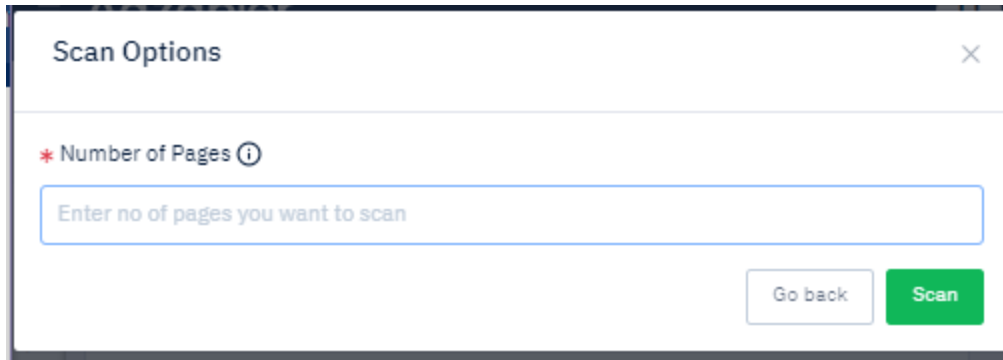
8. After filling all the fields duly, click Validate.

Scan and Results

1. Once you fill out the Scan Behind Login form and validate, then click Scan Now. The Scan Options appear.

Scan Options   ✕

      Quick Scan   Deep Scan

                                          Close

2. If you want to scan up to 10 pages of your domain, select Quick Scan. Or if you want to scan more pages, select Deep Scan.

1. Enter the number of pages to be scanned and click Scan.
   The scan process starts.
   When the scan is in progress, it shows the Scan Status as "Running" and the percentage of completion on the progress bar. Once the scan is completed, the status will show "Completed".
   After completion of the scan, the pie chart analytics of scanned details also appear on the window.
2. Go to the Cookie Category page to view the scanned cookie details.
   For more details, see *Cookie Categorization*.

Cookie Consent Events

You can include the following functions in your website code when you implement Adzapier's cookie banner on your website.

- Initialization

- Open cookie preference (privacy settings) pop-up

- Get Consent Activity

- Get Consent Information

- Get Consent Status

Initialization

The function given below calls once the cookie banner application is initialized on your website.

```
window.addEventListener('OnConsentInit', (e) => console.log(e.detail));
```

Open Cookie Preference (privacy settings) Pop-up

When the user clicks Privacy Settings on the cookie notice or clicks the consent badge on the window, the preference pop-up opens by calling the below functions

If you are using version 1, then use the below function

```
window.AzCMP.onOpenPopUp();
```

If you are using Version2, then use the below function

```
window.AZCookieConsent.onOpenPreference();
```

Get Consent Activity

When the user provides any consent using the cookie banner, the event will return a value, and the same can be viewed by calling the below function.

```
window.addEventListener('OnConsentInit', (e) => console.log(e.detail));
```

An example is given below:

```
▼{device_id: '9d8a059b-eec0-48ff-906a-fbf1f2c3c513', consentVersion: 4, pageViews: 18, essential: true, functional: false, …} ⓘ
    LastPublishDate: "2022-05-03T12:56:38.129Z"
    advertising: false
    analytics: false
    consentVersion: 4
    device_id: "9d8a059b-eec0-48ff-906a-fbf1f2c3c513"
    essential: true
    functional: false
    lastInteraction: "2022-06-14T15:04:59.539Z"
    pageViews: 18
  ▸ purpose: {essential: true, functional: true, analytics: true, advertising: true, social_media: true, …}
  ▸ purposeIds: (6) ['101', '102', '103', '104', '105', '106']
    social_media: false
    status: "save_setting"
    tcString: "1---"
    type: "GENERIC"
    unknown: false
  ▸ [[Prototype]]: Object
```

Get Consent Details

The detailed information of the consent provided by the user like the consent status, and the purposes opted in and opted out can be viewed by calling the below function.

```
window.AZCookieConsent.onGetConsentDetails();
```

An example console is given below:

```
▼{device_id: '9d8a059b-eec0-48ff-906a-fbf1f2c3c513', consentVersion: 4, pageViews: 18, essential: true, functional: false, …} ⓘ
    LastPublishDate: "2022-05-03T12:56:38.129Z"
    advertising: false
    analytics: false
    consentVersion: 4
    device_id: "9d8a059b-eec0-48ff-906a-fbf1f2c3c513"
    essential: true
    functional: false
    lastInteraction: "2022-06-14T15:04:59.539Z"
    pageViews: 18
  ▶ purpose: {essential: true, functional: true, analytics: true, advertising: true, social_media: true, …}
  ▶ purposeIds: (6) ['101', '102', '103', '104', '105', '106']
    social_media: false
    status: "save_setting"
    tcString: "1---"
    type: "GENERIC"
    unknown: false
  ▶ [[Prototype]]: Object
```

Get Consent Status

It returns the status of the consent given by the user.

```
window.addEventListener('AzConsentStatus', e => { console.log(e.detail) })
```

An example status is given below:

```
▼{status: 'init', show: true} ℹ
    show: true
    status: "init"
  ▶ [[Prototype]]: Object
```

Scheduled Scan

With your Adzapier Portal account, after successfully subscribing to a Cookie Consent plan, and assigning desired property under the plan to the subscription, you can scan for cookies from the domain. Now the scan can be scheduled based on your needs and the type of plan(Stater, Essential, Professional, and Enterprise) you have purchased. If you schedule a scan, it will occur automatically on the same day and time each month that you specify. Our goal in creating this feature is to simplify your life.

To perform a scheduled scan you have to enter the date without the month or year, for example- 30. If you enter the date as 31, there is a possibility that the scheduled scan won't take place if the month doesn't have 31 days. So, it is advised to choose a date from 1 to 30.

Follow the steps to schedule a scan for your domain

1. On your account home page, in the menu bar, click the organization & property selector menu.
   The list of organizations with the properties appears.
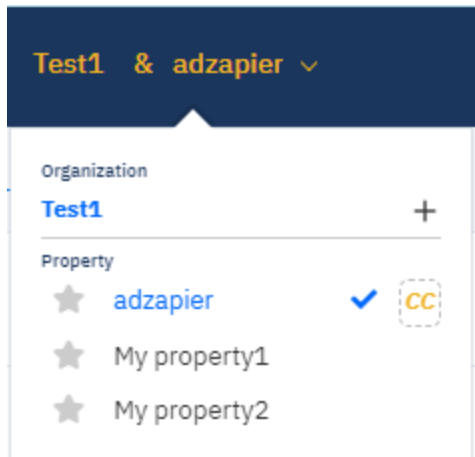
2. Select the property for which you want to schedule a scan.

3. In the Cookie Consent menu, click Cookie Scanner.
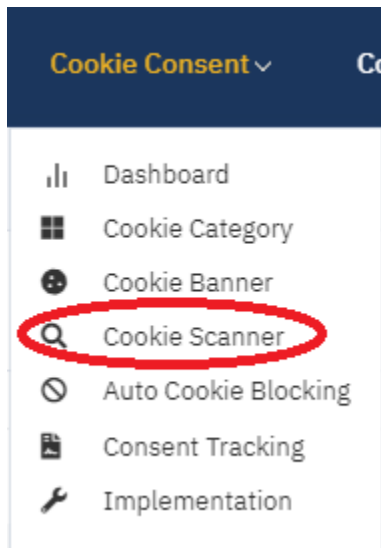
The Scanning Details page appears.
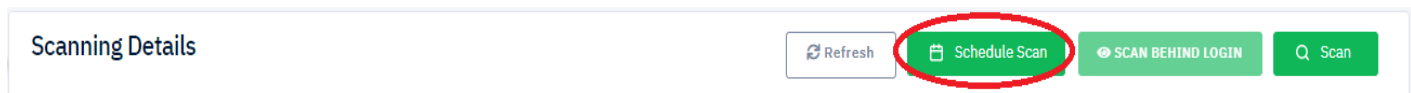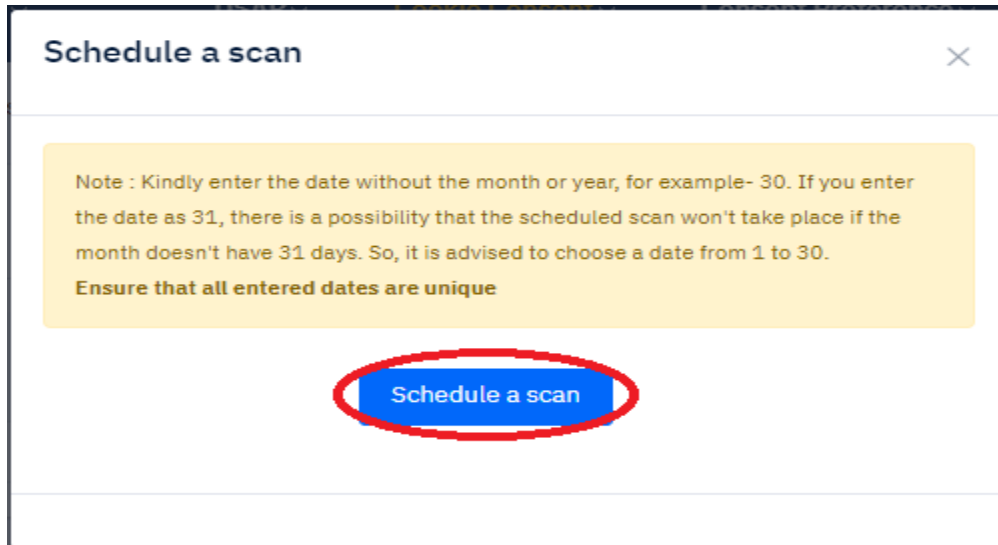
4. Click Schedule Scan
   The Scheduled Scan page appears.
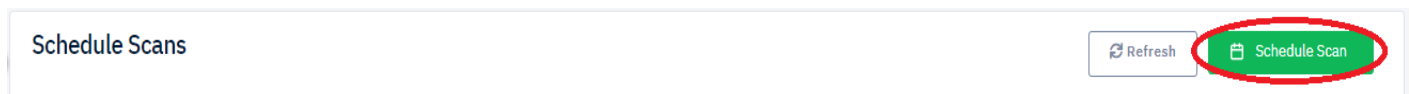
5. Click Schedule Scan
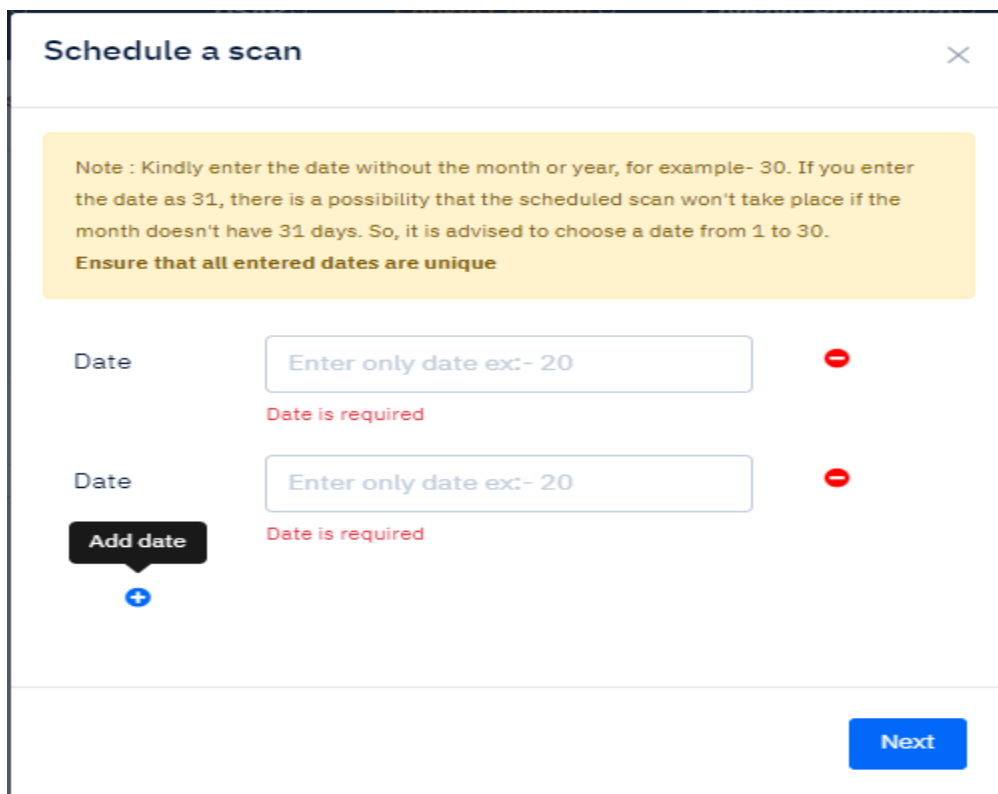   A pop-up of scheduled a scan appears. Click Schedule a scan.

6. Add dates in accordance with the pop-up note. You can add two dates to the Starter and Essential plans and five dates to the Enterprise plan according to the scan availability. You can add as many dates to the Enterprise plan.
   Click on Next.

7. Scan Option pop-up appears. If you want to scan up to 10 pages of your domain, select Schedule scan with the default no of pages. Or if you want to scan more pages, select Schedule scan by entering the number of pages.

8. Enter any no of pages and click Schedule.

9. Then List of Scheduled scans page appears.

Schedule Scans

<div>Refresh | Schedule Scan</div>

Scan Id	Date of scheduled scan	Max pages	Created At	Updated At	Edit	Delete
b1d03217-331f-49bd-9b1...	20	15	2022-12-14	2022-12-14		
db53e563-19a2-4b1f-8cee...	15	15	2022-12-14	2022-12-14		

10. Click to edit any scheduled scan details. You can change the Date of the scheduled scan and the number of pages then click update.

Update scheduled scan date and pages

Date of scheduled scan :

```
20
```

Number of pages :

```
15
```

Update

11. Click to delete any scheduled scan. A confirmation pop-up appears. Click Yes if you want to delete the scheduled scan otherwise click No.

Confirm

⚠ Are you sure you want to delete this scheduled scan?

✕ No   ✓ Yes

12. A toast message stating "Schedule has been deleted successfully" will display.