onetrust

Cookies Consent Expert

Certification Program Handbook

Privacy & Data Governance

DISCLAIMER:

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue.

The training environment provided to you is only for use during the OneTrust Certification Training Program. You will only have access to login for the duration of training.

Training URL: training.onetrust.com

Please refer to your instructor for the password to your environment.

Contents

OneTrust Cookies Consent Expert Certification Program Reference Guide

Prepared for:

OneTrust Cookies Consent Expert Certification Attendees

Version 202209.2.7

Resources & Support

Sales

- Email: Sales@onetrust.com
- Phone Numbers:
    - *London:* +44 (800) 011-9778
    - *Atlanta:* +1 (844) 228-4440
    - *Munich:* +49 (175) 371-2983

Technical Support

- Email: support@onetrust.com
- Phone Number: +1 (844) 900-0472

Partner Support

- Email: partnersupport@onetrust.com

This partner support can assist with:

1. Scheduling Client Demonstrations
2. Submitting an RFI/RFP with OneTrust
3. Client Referrals
4. Account Strategy & Alignment
5. Additional Resources & Collateral

Other resources include:

1. Product Demonstration Videos
2. OneTrust Overview Brochure
3. How OneTrust Helps with GDPR Whitepaper
4. SmartPrivacy Workshops Registration
5. OneTrust Pricing Model

MyOneTrust

- Website: my.OneTrust.com

My OneTrust is a platform that can be accessed by all OneTrust customers for additional resources which include, but it not limited to:

1. OneTrust Knowledge
2. Release Notes
3. Schedule Maintenance
4. Live System Status
5. Submit a Ticket
6. Developer Portal
7. Get OneTrust Certified

Tenant Support Request

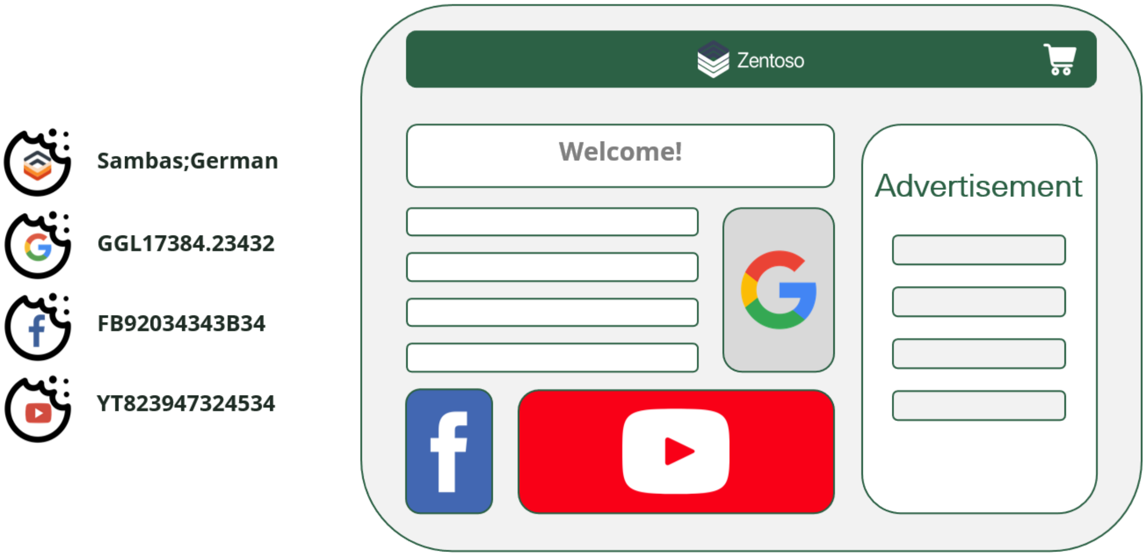
You can submit a support desk ticket directly to the OneTrust Support Team through your tenant by following these steps:

1. Log into OneTrust
2. Click the Launch Pad in the top left corner
3. Click "Get Help" in the bottom right of the menu
4. Use the knowledge portal to search for solutions
5. If no solutions are found, click the "Contact Us" button
6. Fill out your inquiry in the message portal that appears
7. Click "Send"

Key Terms & Concepts

Cookies

Cookies are text files that websites place on a user's device, such as a computer, tablet, phone, etc. that contains various information. This information can then be read by that or other websites later to be used for different purposes. For example, let's take this Zentoso website below:



When joining this website, a user may select which language they'd prefer to read the information in, such as German. This preference is saved by a cookie so that, upon visiting the website at a later time, it'll know to present the data in German without needing re-ask the website visitor.

Meanwhile, to enhance their user experience on the website, Zentoso is using a Google Analytic cookie to track click paths from one website page to another to gain information on how users actually navigate their website. This information can then be used later to make enhancements to the site.

Many websites contain connections to social media sites like Facebook, LinkedIn, Twitter, or more. These allow visitors to click that button to automatically log into their social media to share any articles, blogs, or more from the site. This login credential memorization by the system is performed by cookies.

Finally, there may be some functionalities on the site, such as personalized YouTube videos. This is another example of how cookies can be used to personalize the functionality of a website to the specific user.

Cookie Classifications

Since cookies then invention of cookies in the 1990s for the purpose of remembering which goods to sell on ecommerce websites, their uses have expanded greatly. With these changes come new classifications. There are two main areas that help classify cookies into different categories: origin and duration.

Origin

Origin classifications specify from where the cookie got placed onto a user's device from.

- First Party – Cookies that are placed on a device by the website that the user is visiting.
    - If a user visits www.onetrust.com and www.onetrust.com places a cookie onto the website visitor's computer, that would constitute a First Party Cookie.
- Third Party – Cookies that are placed on a device from a website *other* than the website being visited
    - If a user visits www.onetrust.com and a cookie is dropped from a social media login button, embedded video from elsewhere than OneTrust, or an advertisement, for example, those would all be Third Party Cookies.

Duration

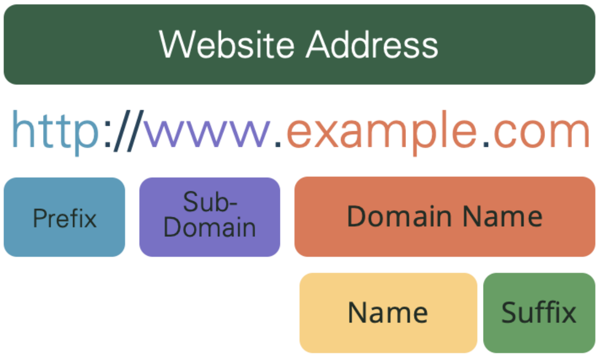
Duration classifications specify how long a cookie stays on a user's device.

- Session – Cookies that are only stored on the device for as long as the browser remains open
    - As soon as a user closes out of a tab or browser, the cookies associate with that tab or browser are deleted from the user's device.
- Persistent – Cookies that remain on a device longer than when a tab or browser is closed and can be recognized when a device re-opens the browser or app later.
    - Length can be any set amount of time – decision is up to the cookie developer

Domains

Postal addresses in the United States consist of a number, street, city/town, state, and postal code. Each individual piece will not identify a single, specific location to deliver mail. 123 Example Street, Atlanta, Georgia 12345, however, will.

Website domains are similar. These domains act as a unique identifier for users to access a specific website that are built from smaller, broader, individual pieces, as seen below:



What's Included in Website Scans

OneTrust's Cookies Consent module includes a website scanner that looks through all pages of a user-determined website to review all cookies of all classifications that will drop onto a device. To do that, the user in OneTrust must specify the website address to scan. This is usually done by only scanning at the Domain Name level. The reason for this is because websites may have many website addresses, for example:

- www.onetrust.com
- training.onetrust.com
- sales.onetrust.com
- support.onetrust.com
- my.onetrust.com

Scanning www.onetrust.com would only search cookies on the first bullet point on this list but ignore all the other sites and pages listed below that. If a user scans only onetrust.com without any subdomain, all subdomains are included and all of the bullet points listed above are included.

To practice, determine which of the following would be scanned if a user enters in "zentoso.com" into the website scanner:

- www.zentoso.com/shop
- Blog.zentoso.com
- www.zentoso.de

- www.zentososhop.com
- www.zentoso.com/uk

Answers with reasoning in middle of next page.

Domain	Included?	Excluded?	Reasoning
www.zentoso.com/shop	X		The base domain of zentoso.com includes all subdomains (www) and pages (/shop)
Blog.zentoso.com	X		Because no subdomain was specified in the scan, the subdomain of "blog" will be included.
www.zentoso.de		X	The .de suffix creates a different domain than .com
www.zentososhop.com		X	Zentososhop.com is different than just zentoso.com
www.zentoso.com/uk	X		The scan will include all pages of the zentoso.com domain

Regulation Overview

ePrivacy Directive

Article 5(3)

The ePrivacy directive came about in 2002 and, though it wasn't a binding law, gave guidance to all member states in the European Union on how to handle and protect data. This directive's focus is on the "Confidentiality of Communications."

Summary

Article 5 Section 3 deems that a user's consent must be obtained by an organization before cookies can be stored or used "on a user's terminal equipment." This means that organizations should create a process to collect and track consent for the different types of cookies that their websites will place on a user's device, whether computer, phone, tablet, or other.

Scope

This consent must be gathered for all cookies except those that are strictly necessary for the organization to provide their service. For example, cookies were invented in the 1990's for ecommerce websites to remember what was added into the shopping cart to sell and ship the appropriate goods as per the website visitor's direction. Because the organization would not be able to sell these goods without those cookies tracking that information, this is a strictly necessary cookie. Any cookies that are not used in these imperative types of ways by the organization would require consent.

Other Requirements

Beyond the collection of consent, individuals need to know what it is they're consenting to. This means that the information about the cookies a website are placing and reading on an individual's device needs to be communicated clearly and comprehensively to the person giving consent.

General Data Protection Regulation (GDPR) – Article 7

Summary

Article 7 of the GDPR focuses conditions for consent. According to the GDPR, organizations must be able to prove that they've collected proper consent from data subjects. When proving that consent has been collected, the validity of that consent must also be demonstrated.

Scope

This demonstration of consent applies in all scenarios where consent is required. From a cookies' perspective, this means that the demonstration of proper and valid consent must be had by organizations for all cookies outside of those that are strictly necessary.

Other Requirements

Proper or valid consent has several aspects, including:

- Clearly distinguishable (purposes for consent aren't hidden within length terms and conditions)
- Intelligible (understandable to the intended audience)
- Easily accessible
- Uses clear and plain language
- Provide opportunities for consent withdrawal
    - Must be just as easy to withdraw consent as it was to give
- Performance of a contract cannot be conditional on consent if the processing is not necessary for the contract

General Data Protection Regulation (GDPR) – Article 21

Article 21 focuses on the data subject's right to object.

Section 2

"…where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time."

Cookies are often used for direct marketing purposes. These types of cookies are referred to as Targeting, Marketing, or Advertising cookies. They track a user's browsing history and then advertise to that user based on what the site determines to be relevant due to the information on that data. Because of this, users under the jurisdiction of the GDPR have the ability to object or opt-out of this type of processing at any time. This is done through DSAR webforms, Cookie Preference Centers, or a "do not sell" my information button.

Section 3

"…where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed."

GDPR's Article 21 Section 3 continues to say that if a data subject does decide to opt out of processing for direct marketing purposes, that the organization must obey those wishes. So if targeting cookies are opted out of, organizations can no longer drop those types of cookies onto their devices or read any previous dropped targeting cookies that are already on their devices.

Glossary

Active - Cookies will be set unless and until the visitor opts-out of this group. This is the initial status for groups with the Implied Consent model.

Always Active - Use this where you do not want to give visitors control over these cookies. The Strictly Necessary group is Always Active by default and cannot be changed.

Cookie - Text file stored on a client machine that may later be retrieved by a web server. Allows web servers to keep track of user’s browser activities and connect individual web requests into a session.

Do Not Track - If the user’s browser sends a DNT=1 header (request not to track), cookies will not be set unless the user changes their preference in the interface. If the DNT header is not received, or is set to 0, then the group is ‘Active’ and cookies will be set.

Domain - Unique identifier address where users can access a specific website.

First Party Cookie - Cookie placed by the website visited.

Inactive - Cookies will not be set until visitors actively allow them. This is the initial status for groups with the Explicit Consent model.

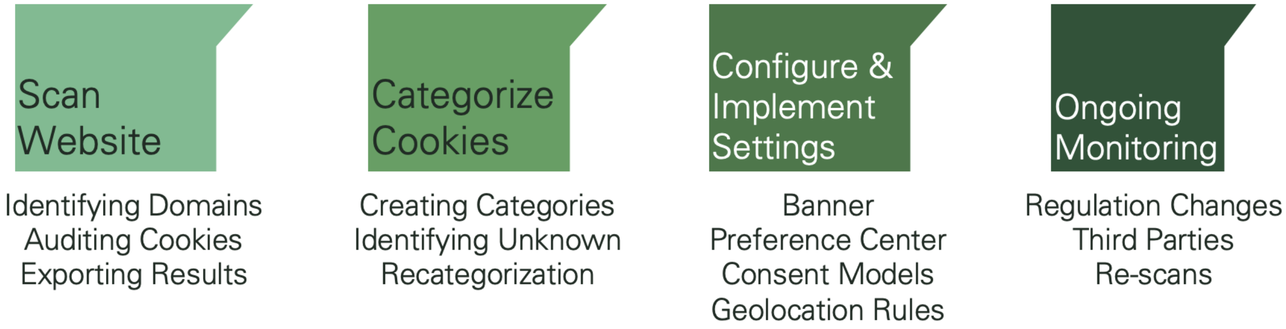
Inactive Landing Page - Cookies will not be set on the first page but set automatically when the user navigates to a second page or reloads the first page. This is the initial status for groups with the Soft Opt-in model.

Persistent Cookie - Cookies with a defined lifespan set by the developer of the cookie

Session Cookie - Cookies stored only as long as the browser is open

Third Party Cookie - Cookies placed by a party other than the website visited

Execution



Scan Website

Identifying Domains
Auditing Cookies
Exporting Results

Categorize Cookies

Creating Categories
Identifying Unknown
Recategorization

Configure & Implement Settings

Banner
Preference Center
Consent Models
Geolocation Rules

Ongoing Monitoring

Regulation Changes
Third Parties
Re-scans

Overview

Scan Website

Using OneTrust's website scanner is incredibly important, as it will inform the organization on which cookies are being place onto visitors' devices from their website. From there, companies can take best next steps, which will be covered in future exercises.

The website scanner can be limited in several ways, including:

- Website URL – inputting specific sub-domains, such as www, will limit the scan to those subdomains
- Limit Scan – limits the total number of website pages scanned to a specified amount
- Query Parameters – limits scan to specified parameters, such as only pages with a specific language
- Target Pages – will prioritize certain pages over others to ensure they're included in the scan
- Sitemap – uses provided site map to scan website

Step 1: Select Launch Page and Cookie Consent

Step 2: In the Digital Properties section, click the Websites tab on the left

Step 3: Click the blue 'Add Website' button to run a new scan

Step 4: Add the URL 'onetrust.com'

Step 5: Limit scan to 5 pages

Step 6: Select 'Scan Only'

Step 7: Repeat the steps and add 1 more URL of your choice

Build Cookie Banner Template

The Cookie Banner and Preference Center allow organizations to give data subjects/consumers the ability to opt in or out of different types of cookies. This information is presented in an easily accessible, easily-understood form, meeting the requirements that are specified in the Regulations section.

When building out these Cookie Banners and Preference Centers to meet your organization's needs, you're able to customize:

- Text
- Links
- Colors
- Layout
- Language
- & more

Step 1: Go under **Setup** and select **Templates**
Step 2: Select the blue **Add New** button
Step 3: Select the **GDPR Template** and then select the blue **next** button.
Step 4: Name this the 'Training Template Banner' and set the organization as "OneTrust'
Step 5: Default language, select a language of your choice
Step 6: Select the blue **Create Template** button
Step 7: To the left side of the screen select **Layout** and choose your option
Step 8: Then change the banner colors in the **Styling** section
Step 9: After styling, edit the Title & Description in the **Content** section
Step 10: Select the **Save Template** button at the top right of the screen
Step 11: Select the white **Manage Languages** button on the right
Step 12: Check the box next to the preferred language
Step 13: Select the blue **Save** button

Define Geolocation Rule

Understanding Geolocation Rules

Due to varying regulations around the world, Cookie Banners and Preference Centers will need to behave differently based on where a website visitor is tuning in from. This is where Geolocation Rules come into play. Geolocation Rules can be created for region to region to specify the behavior of the Cookie Banner and Preference Center. These differences in behaviors are what's called consent models, detailed further in the next section.

Similar to how single Banner and Preference Center templates can be used for multiple domains, a single Geolocation Rule can behave the same.

Understanding Consent Models

There are 5 main consent models that can be configured in OneTrust, each with their own level of technical implementation intensity. The 5 are detailed below, starting from least to most intensive:

1. Notice Only – websites initially place all cookies on the visitor's device, shows a notice that they're doing so, then there's no further action possible by the visitor.
    a. Seen often in the United States
2. Do Not Track – tracking preferences are determined via the website visitor's browser settings
3. Opt-Out Consent – websites initially place all cookies on the visitor's device, the Cookie Banner is shown, then the visitor can opt-out of specific types of cookies being placed. If/When they opt out, the organization can no longer read those types of cookies.
4. Implied Consent – websites initially drop on Strictly Necessary cookies on the visitor's device, the Cookie Banner is shown, if the user ignores the Cookie Banner completely the website assumes that means consent is given and will place the remaining types of cookies on the device.
    a. Often used in California
5. Opt-In Consent – websites initially drop only strictly necessary cookies, Cookie Banner is shown, website will only drop remaining cookies if website visitor chooses to opt-in to the rest of the cookies with an affirmative action
    a. Seen often in the European Union
    b. Affirmative action means the user actually does something (clicks a button, fills out a profile, checks a box, etc.)

Configuring a Geolocation Rule

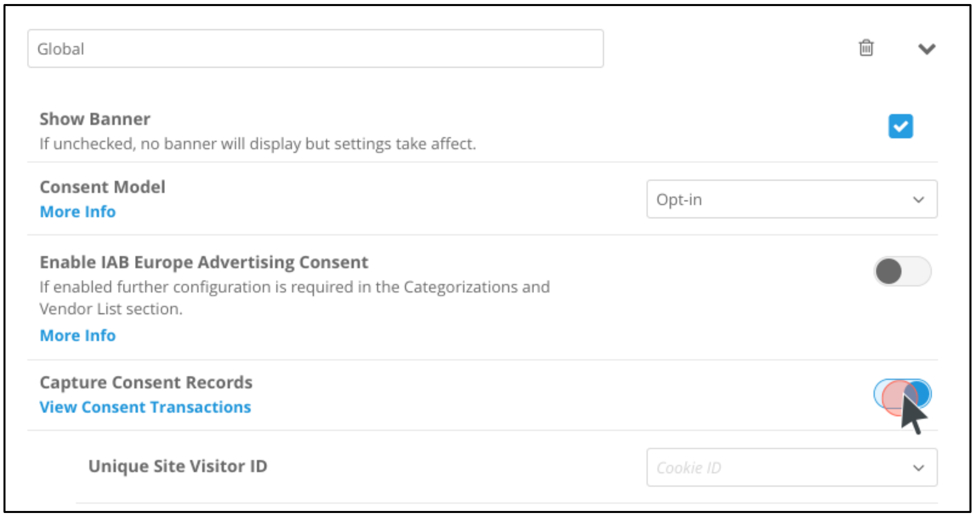
When configuring a Geolocation Rule, there's two types of rules that will be configured:

- Regional – the consent models determined in these types of rules will only apply to the region specified in that rule
- Global – any region that is not specified in a regional rule will use the consent model specified in this rule

Step 1: Select the **Geolocation Rules** tab under the Setup section
Step 2: Select the blue **Create New** button
Step 3: Rule Group Name: **Training Geolocation Rule**
Step 4: Make the Organization **OneTrust**
Step 5: Description will also be: **Training Geolocation Rule**
Step 6: Select the blue **Create** button
Step 7: Click **Edit Pencil** to the right of 'Default'
Step 8: Remove the **GDPR Template** and change it from the drop down to **Training Template Banner**
Step 9: To the right of **Cookie Categories**, change Opt-in to **Custom**
Step 10: Select the carrot to the right and change the consent model of different Cookie Categories
Step 11: Select all 3 checkboxes in the **Close Banner** behaviours section
Step 12: Select the **Save** button
Step 13: Click the white **Add Rule** button at the top right
Step 14: Rule Name: EU Rule
Step 15: Select EU region in the dropdown menu
Step 16: Remove the GDPR Template and select the **Training Template Banner** from the dropdown menu
Step 17: Uncheck all Close Banner Checkboxes in the Behaviours section
Step 18: Click **Save**
Step 19: Select the **Assigned Domains** tab at the top
Step 20: Click **Assign to Domains** on the right
Step 21: Check all the boxes for the previously scanned websites
Step 22: Click **Save**

Consent Logging

Consent Analytics for cookie preferences can be pulled in via user choices into the Cookies dashboard. This will help track items such as how many visitors you had and the consent will be segmented out by type and purpose. Consent will also be tracked as Consent Receipts/Transactions in the Consent module. In order for this feature to be used, this setting at the bottom of Geolocation Rules must be toggled on:



Global

Show Banner ☑
If unchecked, no banner will display but settings take affect.

Consent Model — Opt-in
More Info

Enable IAB Europe Advertising Consent ○
If enabled further configuration is required in the Categorizations and Vendor List section.
More Info

Capture Consent Records ●
View Consent Transactions

Unique Site Visitor ID — Cookie ID

Scan Results & Login Blockers

Cookie Categorizations

There are 5 default Cookie Categories in OneTrust. When the website scanner is complete, it will categorize as many cookies as possible within one of these 5 categories. Any cookie that was unable to be categorized will require manual categorization, covered in the next exercise.

Cookie Category	Description	Example
Strictly Necessary	Essential for organizations to provide their good or services to the data subject/consumer.	Remembering what was added to shopping cart to sell proper goods.
Performance	Used to understand visitor behavior to improve UX of website	Tracking click paths, website speed, etc.
Functional	Improve website functionality and personalize experience	Remembering visitors' preferred languages, embedding videos, etc.
Targeting	Track browsing behavior to personalized advertisements	Visitor shops for baby clothes so advertisements are for baby supplies
Social Media	Cookies specific to creating ease in using social media	"Share to" buttons that log you into Facebook, Twitter, LinkedIn, etc.

Login Blockers

When reviewing scan results, they may seem incomplete. A major contributor to this is because the blocker may have been blocked by a feature on the website. There are two types of blockers:

1. Authentication
   a. These are items such as age verifications or Terms and Conditions in need of acceptance
   b. Acceptance to these types of blockers are done via cookies. To bypass these blockers, you'll need to load the system with the correct cookie values for the scanner to use in order to get to the next page
      i. For example, there may be an age verification cookie (age_ver) that's checking to see if someone is over the age of 18. If they are, the cookie value is 1, if they are not the value is 0. You can input this information on the website scan results page to rescan to capture that page.
2. Login Pages
   a. These are items such as username and password logins, filling out a webform, etc.
   b. To bypass these types of blockers, you'd recreate the webform fields via inputting the html in the website scan results page to let the system know what the webform will look like. For each field, you'd also input the html that you want the scanner to read in each field in order to log in and scan the next page.

How to Review Scan Results

Step 1: On the left side of the screen, select **Websites**
Step 2: Select a previously scanned domain whose status is Completed
Step 3: In the **Scan Results** tab review specific cookie Hosts, Name and Details
Step 4: Select the white **export** button on the top right.
Step 5: Then select the blue **Export** button again to confirm what scan you'd like to export
Step 6: Select the **Bell Icon** at the top
Step 7: Select Download Scan Result
Step 8: Open downloaded file and inspect cookie category tab

Categorizations – Assign Cookies

Cookiepedia will categorize most of the cookies found by the website scanner, but not all of them. Cookies that were unable to be categorized will be in the results as "Unknown." This can cause issues because if an Unknown cookie *should* be Targeting, for example, then it will still drop onto a visitor's device even if they opt-out of Targeting cookies, since the system didn't associate that specific cookie as Targeting. This, of course, can cause organizations to be non-compliant. This exercise is to show how to categorize these Unknown cookies as one of the 5 categories we reviewed in the previous exercise.

Step 1: On the left under 'Setup' select **Categorizations**
Step 2: Select the **cookies** tab at the top
Step 3: Select the filter icon at the right, Select the blue **Add Filter** button, Field: Default Category, Operator: Equal to, Field Value: Unknown, then select the blue **Apply**
Step 4: Select several cookies, then select the white **'Recategorize'** button, and select **Strictly Necessary** cookies.
Step 5: Select **Categorize**

Categorizations – Create Categories

Though OneTrust comes with the 5 default categories, more can be created. Whether out of the box or custom, each category can be updated. For example, Strictly Necessary cookies can be renamed to Essential cookies. This name change will update all Cookie Banner and Preference Center templates, as well. Another key field that should be reviewed at this time is the ID. This ID will be a critical part of ensuring that the technical integrations are working properly.

Step 1: On the left under 'Setup' select **Categorizations**
Step 2: At the top, you want to select the 'Categories' Tab
Step 3: Select the blue **Create Category** button to the right of the screen.
Step 4: Category Name: **Optional Cookies**, ID: **C6**, Add a Description of your choice
Step 5: Click the blue **Create** button
Step 5: Select each **Category** on the left and click the white **Edit Category** button to change each category ID from C0001 to C1, C0002 to C2, etc.
Step 6: Click **Save** for each update you make

Website Script Integration

Create Basic Website

Now that all of the front-end configuration has been done in OneTrust, it’s time to test that what we’ve configured is what we want. To do this for training, we will first build our own basic website.

Step 1: Open a new text file in (Notepad for Windows or TextEdit in Mac)

Step 2: Ensure the format is **Make Plain Text**

Step 3: Enter the necessary code:

```
<html>
<head>
</head>
<body>
OneTrust is the Best!
</body>
</html>
```

Step 4: Save file as: **index.html**

Step 5: Open saved file

Integrate Cookie Script

Now that we have a basic website built, we are able to integrate our Cookie Banner and Preference Center, which will bring in all the consent models and customizations along with it. To integrate this information, which is done by placing scripts into our website’s code, there’s a few concepts we first need to understand.

Scripts/CDNs

Once all front-end configuration is done, there are two scripts or CDNs (Content Delivery Network) that can be published and used, each with their own specific purpose.

- Testing – this script should be used when making the decision on whether the configuration is as expected or not
  - **Pro:** Updates get pushed to the testing script immediately after publishing, allowing you to quickly adjust to meet your needs
  - **Con:** The speed at which the Banner/Preference Center renders on the website is slower
- Production – this script is used on the actual website(s) after all configuration is deemed correct
  - **Pro:** The rendering speed on the website is practically instantaneous
  - **Con:** Any updates to configuration take anywhere from 4-24 hours to push to OneTrust after being published

Any changes that are made in OneTrust to the consent models, Geolocation rules, Cookie Banners and Preference Centers, etc. will require a user to re-publish these scripts. Publishing doesn't create a new script that needs to be put into the website code, it just confirms that the already-integrated script should now be using the latest configuration.

Identifying Language Preference

User language preferences will also need to be determined to know how to present the Cookie Banner and Preference Center. There are three ways this can happen:

- Browser Settings – a user's preferences in the browser (such as Google Chrome) are used
  - This is the default method
- HTML on Page – the html class on a webpage's code can specify what language to use
- Custom Deploy – you can specifically tell the system which language to use on which domain-level websites
  - OneTrust.com → English
  - OneTrust.fr → French
  - OneTrust.de → German

How to Integrate Scripts

Step 1: One the left side, under Integrations, select **Scripts**
Step 2: Select a previously created domain
Step 3: Click the **Test Scripts** tab at the top
Step 4: In the Testing CDN section select **Copy Scripts**
Step 5: Click **Publish Test** and then **Confirm**
Step 6: Select **Publish Test Scripts** and then Cancel the live Preview.
Step 7: Open your notepad or textedit with the index.html file
Step 8: Paste copied **CDN script** in between <head> and </head>
Step 9: **Save** the file
Step 10: **Refresh** opened index.html webpage to reveal the Cookie Banner
Step 11: Go back to the OneTrust tool and scripts
Step 12: In Do Not Sell & Cookie Setting Button section, click **Copy Scripts**
Step 13: Open the Notepad or TextEdit index.html file
Step 14: Paste copied Do not Sell and Cookie Setting Button script between </body> and </html>
Step 15: Save File
Step 16: Refresh opened index.html page to reveal Cookie Settings button.

Cookie Blocking & Testing

Methods of Blocking Cookies

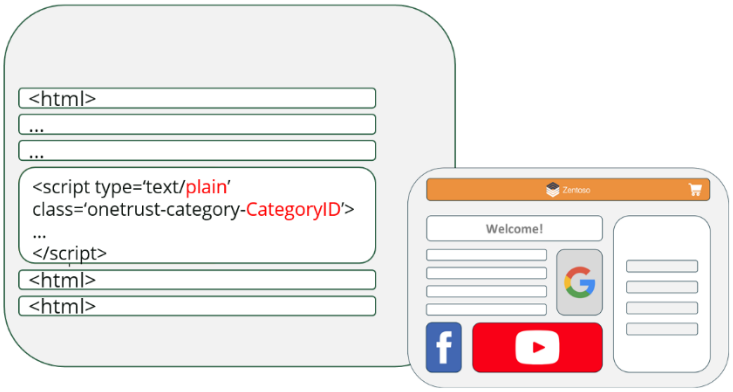
There are three main methods in which cookie blocking can occur:

1. IAB (Interactive Advertising Bureau) Frameworks
2. Tag Managers/Content Management Systems
   a. Much more general and integration information can be found on my.OneTrust.com
3. Auto-Blocking
   a. This allows OneTrust scripts and CDNs to do a lot of the blocking automatically
      i. Pros:
         1. A bit easier
         2. Not as labor intensive if development resources aren't as readily available
      ii. Cons:
         1. OneTrust controls the client's webpage and our CDNs will control what scripts are activated
         2. Higher risk for cookies to not be categorized correctly
4. Script Rewrite
   a. Manually tedious but best way to ensure cookies will be blocked
   b. Can be done in 2 ways:

Editing JavaScript in website code to include OneTrust Cookie Category ID:

-“javascript” becomes “plain”

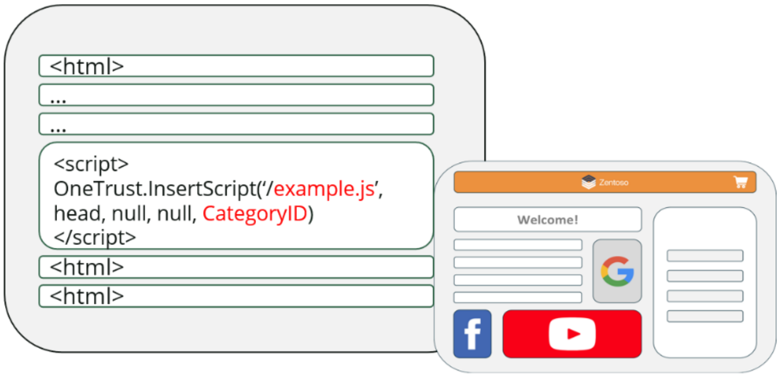
- Cookie Category ID specified



```
<html>
...
...
<script type=‘text/plain’
class=‘onetrust-category-CategoryID’>
...
</script>
<html>
<html>
```

Inserting a JavaScript script that has the cookie JavaScript name and associated category IDs within

- This will use a function called **Optanonwrapper** that will take the user preferences, run through all of the cookies on the website, compare Cookie Category IDs to what they Opted in or out of, then block those cookies that were opted out of.



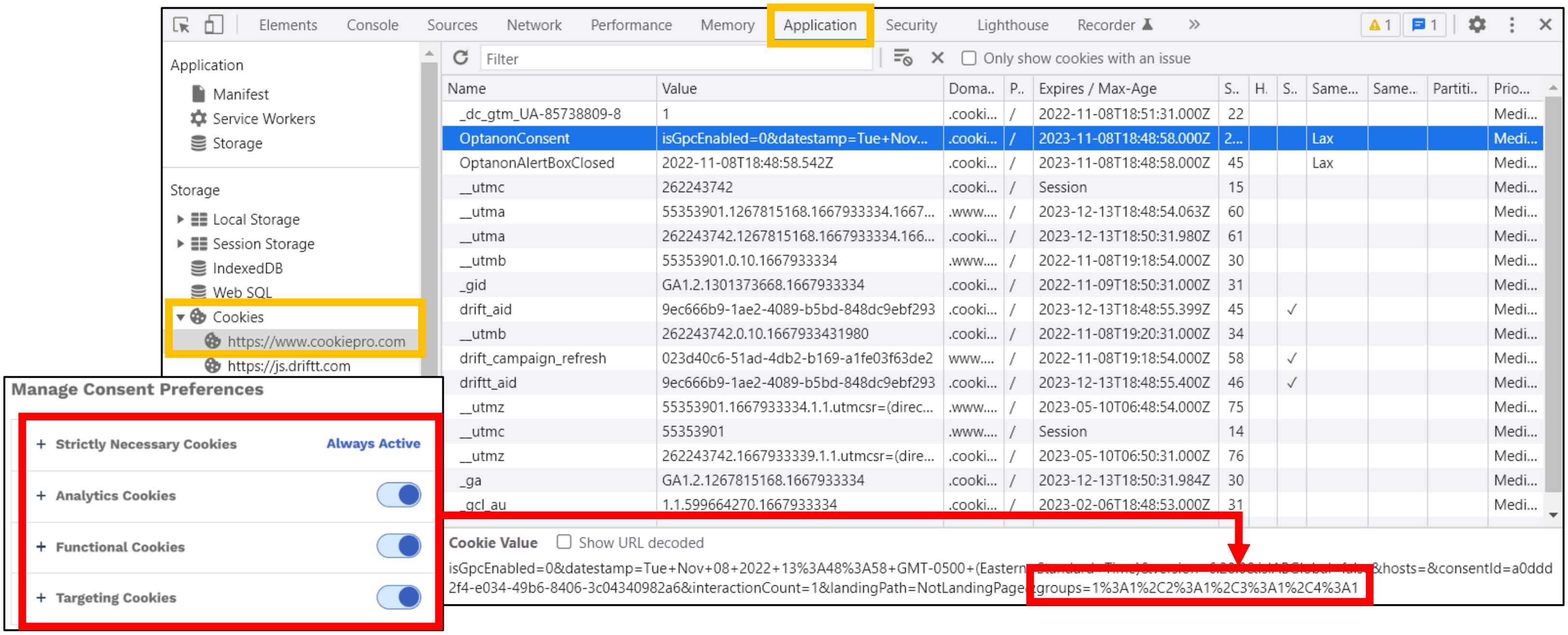
```
<html>
...
...
<script>
OneTrust.InsertScript(‘/example.js’,
head, null, null, CategoryID)
</script>
<html>
<html>
```

Validate Cookie Script

Step 1: Go to cookiepro.com
Step 2: Right-click on webpage
Step 3: Click **Inspect** in the menu
Step 4: Select the **Application** tab
Step 5: Select the storage: Cookies tab at the left
Step 6: Inspect dropped cookies
Step 7: Close inspection window
Step 8: Interact with cookie banner and select **Cookie Settings**
Step 9: Disable Targeting and Analytics cookies
Step 10: Click **Confirm My Choices**
Step 11: Again, inspect the page. Right-click on webpage
Step 12: Click on Inspect in the menu
Step 13: Select **Application** Tab, Select the storage and Cookies tab
Step 14: Inspect **OptanonConsent**

Results can be compared to the screenshots on the next page.

All Cookies Opted Into



Name	Value	Doma..	P..	Expires / Max-Age	S..	H.	S..	Same...	Same..	Partiti..	Prio...
_dc_gtm_UA-85738809-8	1	.cooki...	/	2022-11-08T18:51:31.000Z	22						Medi...
OptanonConsent	isGpcEnabled=0&datestamp=Tue+Nov...	.cooki...	/	2023-11-08T18:48:58.000Z	2...			Lax			Medi...
OptanonAlertBoxClosed	2022-11-08T18:48:58.542Z	.cooki...	/	2023-11-08T18:48:58.000Z	45			Lax			Medi...
__utmc	262243742	.cooki...	/	Session	15						Medi...
__utma	55353901.1267815168.1667933334.1667...	.www....	/	2023-12-13T18:48:54.063Z	60						Medi...
__utma	262243742.1267815168.1667933334.166...	.cooki...	/	2023-12-13T18:50:31.980Z	61						Medi...
__utmb	55353901.0.10.1667933334	.www....	/	2022-11-08T19:18:54.000Z	30						Medi...
_gid	GA1.2.1301373668.1667933334	.cooki...	/	2022-11-09T18:50:31.000Z	31						Medi...
drift_aid	9ec666b9-1ae2-4089-b5bd-848dc9ebf293	.cooki...	/	2023-12-13T18:48:55.399Z	45		✓				Medi...
__utmb	262243742.0.10.1667933431980	.cooki...	/	2022-11-08T19:20:31.000Z	34						Medi...
drift_campaign_refresh	023d40c6-51ad-4db2-b169-a1fe03f63de2	www....	/	2022-11-08T19:18:54.000Z	58		✓				Medi...
driftt_aid	9ec666b9-1ae2-4089-b5bd-848dc9ebf293	.cooki...	/	2023-12-13T18:48:55.400Z	46		✓				Medi...
__utmz	55353901.1667933334.1.1.utmcsr=(direc...	.www....	/	2023-05-10T06:48:54.000Z	75						Medi...
__utmc	55353901	.www....	/	Session	14						Medi...
__utmz	262243742.1667933339.1.1.utmcsr=(dire...	.cooki...	/	2023-05-10T06:50:31.000Z	76						Medi...
_ga	GA1.2.1267815168.1667933334	.cooki...	/	2023-12-13T18:50:31.984Z	30						Medi...
_gcl_au	1.1.599664270.1667933334	.cooki...	/	2023-02-06T18:48:53.000Z	31						Medi...

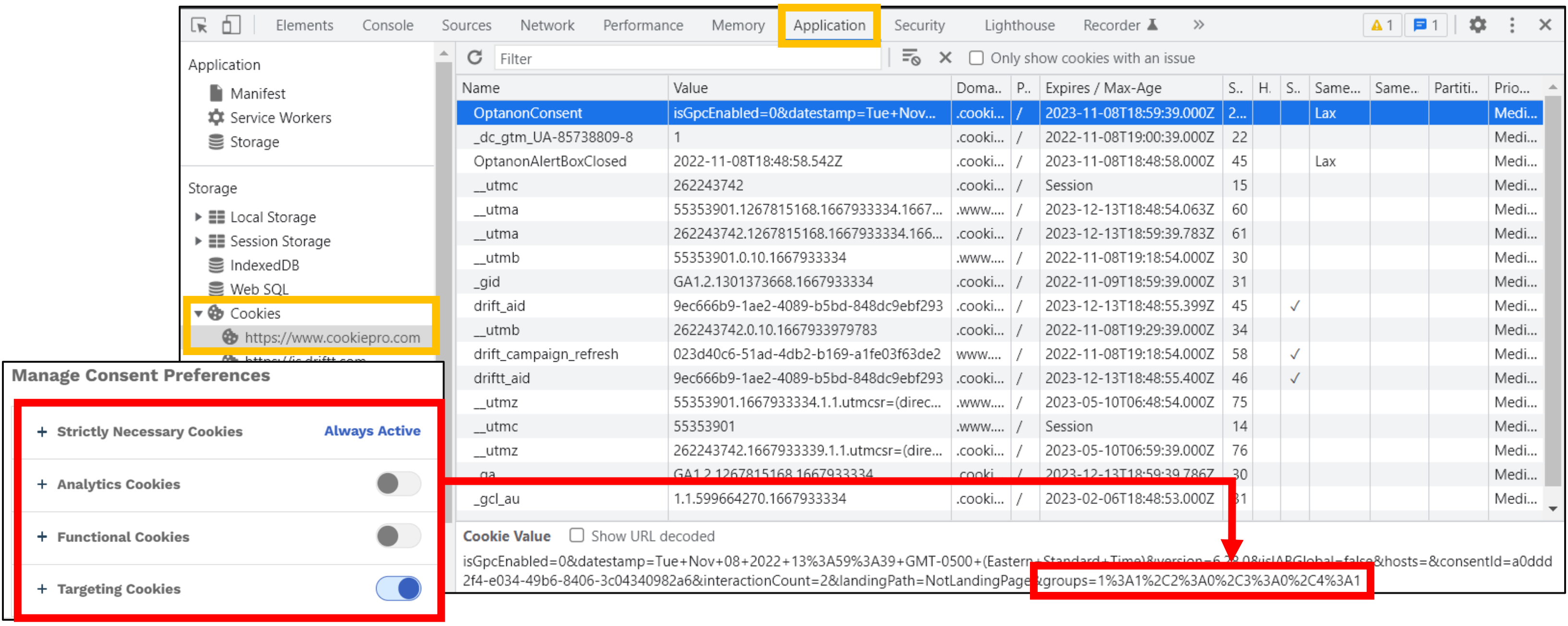
Cookie Value □ Show URL decoded

isGpcEnabled=0&datestamp=Tue+Nov+08+2022+13%3A48%3A58+GMT-0500+(Eastern+Standard+Time)&version=6.28.0&isIABGlobal=false&hosts=&consentId=a0ddd2f4-e034-49b6-8406-3c04340982a6&interactionCount=1&landingPath=NotLandingPage&groups=1%3A1%2C2%3A1%2C3%3A1%2C4%3A1

Manage Consent Preferences

+ Strictly Necessary Cookies — Always Active
+ Analytics Cookies ●
+ Functional Cookies ●
+ Targeting Cookies ●

Targeting & Analytics Opted Out



Name	Value	Doma..	P..	Expires / Max-Age	S..	H.	S..	Same...	Same..	Partiti..	Prio...
OptanonConsent	isGpcEnabled=0&datestamp=Tue+Nov...	.cooki...	/	2023-11-08T18:59:39.000Z	2...			Lax			Medi...
_dc_gtm_UA-85738809-8	1	.cooki...	/	2022-11-08T19:00:39.000Z	22						Medi...
OptanonAlertBoxClosed	2022-11-08T18:48:58.542Z	.cooki...	/	2023-11-08T18:48:58.000Z	45			Lax			Medi...
__utmc	262243742	.cooki...	/	Session	15						Medi...
__utma	55353901.1267815168.1667933334.1667...	.www....	/	2023-12-13T18:48:54.063Z	60						Medi...
__utma	262243742.1267815168.1667933334.166...	.cooki...	/	2023-12-13T18:59:39.783Z	61						Medi...
__utmb	55353901.0.10.1667933334	.www....	/	2022-11-08T19:18:54.000Z	30						Medi...
_gid	GA1.2.1301373668.1667933334	.cooki...	/	2022-11-09T18:59:39.000Z	31						Medi...
drift_aid	9ec666b9-1ae2-4089-b5bd-848dc9ebf293	.cooki...	/	2023-12-13T18:48:55.399Z	45		✓				Medi...
__utmb	262243742.0.10.1667933979783	.cooki...	/	2022-11-08T19:29:39.000Z	34						Medi...
drift_campaign_refresh	023d40c6-51ad-4db2-b169-a1fe03f63de2	www....	/	2022-11-08T19:18:54.000Z	58		✓				Medi...
driftt_aid	9ec666b9-1ae2-4089-b5bd-848dc9ebf293	.cooki...	/	2023-12-13T18:48:55.400Z	46		✓				Medi...
__utmz	55353901.1667933334.1.1.utmcsr=(direc...	.www....	/	2023-05-10T06:48:54.000Z	75						Medi...
__utmc	55353901	.www....	/	Session	14						Medi...
__utmz	262243742.1667933339.1.1.utmcsr=(dire...	.cooki...	/	2023-05-10T06:59:39.000Z	76						Medi...
_ga	GA1.2.1267815168.1667933334	.cooki...	/	2023-12-13T18:59:39.786Z	30						Medi...
_gcl_au	1.1.599664270.1667933334	.cooki...	/	2023-02-06T18:48:53.000Z	31						Medi...

Cookie Value □ Show URL decoded

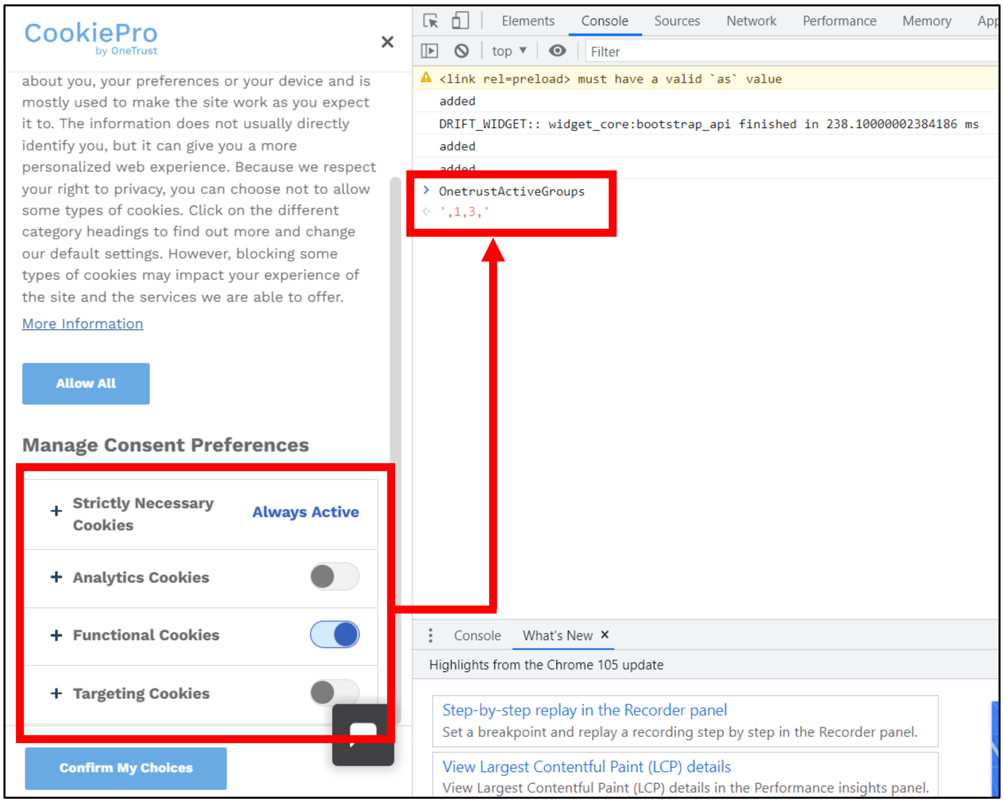
isGpcEnabled=0&datestamp=Tue+Nov+08+2022+13%3A59%3A39+GMT-0500+(Eastern+Standard+Time)&version=6.28.0&isIABGlobal=false&hosts=&consentId=a0ddd2f4-e034-49b6-8406-3c04340982a6&interactionCount=2&landingPath=NotLandingPage&groups=1%3A1%2C2%3A0%2C3%3A0%2C4%3A1

Manage Consent Preferences

+ Strictly Necessary Cookies — Always Active
+ Analytics Cookies ○
+ Functional Cookies ○
+ Targeting Cookies ●

Validate Cookie Settings

Step 1: In the **Application** tab, delete dropped cookies.
Step 2: Reopen **Cookie Settings** in the cookie icon at bottom left of website
Step 3: **Opt-out** of all cookies, except Strictly Necessary
Step 4: Click **Confirm My Choices**
Step 5: Reinspect webpage, **delete** all cookies by OptanonConsent and OptanonAlert
Step 6: In Inspection window choose **Console** tab at the top left
Step 7: Type **OneTrust** where cursor is flashing
Step 8: Select **OneTrustActiveGroups** in the auto-populated drop-down menu
Step 9: Inspect Cookie Categories



about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Manage Consent Preferences

+ Strictly Necessary Cookies	Always Active
+ Analytics Cookies	○
+ Functional Cookies	●
+ Targeting Cookies	○

```
⚠ <link rel=preload> must have a valid `as` value
  added
  DRIFT_WIDGET:: widget_core:bootstrap_api finished in 238.10000002384186 ms
  added
  added
> OnetrustActiveGroups
< ',1,3,'
```

Highlights from the Chrome 105 update

Step-by-step replay in the Recorder panel
Set a breakpoint and replay a recording step by step in the Recorder panel.

View Largest Contentful Paint (LCP) details
View Largest Contentful Paint (LCP) details in the Performance insights panel.