

Google Tag Gateway (GTG) and Consent Management

This document provides guidance on ensuring that STRIGHT's consent management functions correctly on websites that use or are considering using Google Tag Gateway (GTG). It summarizes how GTG works, its impact on Consent Mode, how to verify whether GTG is enabled, and recommended actions when a "late consent signal" is detected.

Note: [STRIGHT supports Google Consent Mode v2.](#)

What Is GTG and How Does It Affect Consent?

Google Tag Gateway (GTG) is a system that delivers Google tags (gtm.js/gtag.js) from your own first-party domain rather than from Google's domain (e.g., googletagmanager.com). This makes the tags less susceptible to ad blockers and browser tracking restrictions (such as ITP/ETP), thereby improving measurement resilience.

However, depending on how GTG is implemented, it may affect consent management. In particular, with one-click injection via a CDN (e.g., an implementation method where you simply toggle a switch to "ON" in the management console of Cloudflare, Akamai, Fastly, etc.), the Google tag script is loaded very early in the page loading process. As a result, you often lose control over the tag's load order, and the Google tag may execute before STRIGHT sets the default consent value (the default consent command).

This phenomenon, where the Google tag fires and reads the consent status before the consent status is finalized, is called a "late consent signal." If a late consent signal occurs, Google may deem that signal non-compliant, which can impact compliance with privacy regulations—including the GDPR—as well as the accuracy of measurement.

Key Point: When implementing GTG via one-click CDN injection, customers often cannot control the script loading order, which is the primary cause of late consent signals.

Official Google GTG Documentation

For more details on GTG, please refer to the following official Google documentation.

- [Google tag gateway guide](#)
- [Google tag gateway with CDN + SGTM](#)
- [Tag Manager consent mode support](#)

The latest URLs and specifications are subject to change by Google. Please check the official documentation above for the most up-to-date information before implementation.

How to Verify if a Tag Is Enrolled in GTG

STRIGHT cannot automatically determine whether GTG is enabled on your site (i.e., whether tags are enrolled in GTG). Please verify this manually using one of the following methods.

Method A: Check in the Google Tag Manager (GTM) dashboard

1. Log in to Google Tag Manager.
2. Click “Admin” in the top navigation bar. Check the container settings to see if there is an entry for “Google Tag Gateway (GTG).” If it is configured, you will see a badge or indicator showing that GTG is enabled.

Method B: Check in the CDN dashboard

- Log in to the management console of a CDN that provides GTG (such as Cloudflare) and open the “Google Tag Gateway” settings page for the target domain. If the toggle is set to ON, GTG is enabled on that site.

Method C: Verify the Delivery Domain and Tag Source

- Use your browser’s developer tools or Google Tag Assistant to verify which domain is serving gtm.js/gtag.js. If they are served from your own domain (e.g., cdn.example.com/gtm.js) rather than a Google domain, GTG is enabled.

Note: Since GTG allows you to change the container filename (the default is gtm.js), searching the source code for “gtm.js” may not yield any results. In that case, please determine the status based on the serving domain.

Action to Take When a Late Consent Signal Is Detected and GTG Registration Is Confirmed

If a late consent signal is detected by STRIGHT’s diagnostics and it is confirmed that the tag is registered with GTG, please take one of the following actions.

Recommended: Adopt Advanced Consent Mode

- Adopt Advanced Consent Mode and enable the following as needed.
- Data Transmission Controls (Data Transmission Controls)
- Global Consent Defaults
- Set the consent defaults appropriately according to your regional requirements (EEA, UK, Switzerland, etc.).

Alternative Options

If the above is not feasible, please consider one of the following:

- Consolidate all tags into a GTM container and deploy GTM via GTG. Migrate to a configuration where the Google Tag Manager container—rather than individual tags—is delivered via GTG.
- Set up GTG manually (manual GTG) to allow you to control the script import order on your end. Switch from one-click CDN injection to a manual configuration that allows you to manage the loading order.
- Google Consent Mode and the Tag Auto Control feature cannot be used together. To prevent duplicate control of

Google-related tags, do not use the Tag Auto Control feature for tag management; use only Google Consent Mode for control.

- When setting the Google Consent Mode tag directly in the HTML, embed it in the following order: 1) STRIGHT Google Consent Mode tag → 2) STRIGHT banner tag → 3) GTM snippet (or Google Global Tag).

Note: While disabling (rolling back) GTG will resolve the late consent signal, doing so will result in the loss of the benefits of first-party measurement provided by GTG. By following the steps outlined above, you can resolve the timing issue while retaining the benefits of GTG.

Why Advanced Consent Mode Is Recommended for Tags with GTG Enabled

Consent Mode Advanced is the recommended consent mechanism for tags with GTG enabled. This is because Consent Mode Advanced is compatible with manual GTG.

In Consent Mode Advanced, Google tags are loaded with the default consent state (typically “denied”) applied at startup. Until consent is obtained, the tag does not set cookies and only sends pings to Google; once the user grants consent, it switches to sending full measurement data.

This mechanism eliminates dependence on the tag loading order, so even if a tag is loaded early due to GTG, it will not collect data as if consent had been granted before consent is actually obtained. In other words, late consent signals are “by design” acceptable.

In contrast, Basic Consent Mode completely blocks tags until consent is granted; therefore, it does not function in GTG environments where tags have already been loaded by a CDN. Consequently, Advanced Consent Mode is recommended for sites using GTG.