cardinal
A Visa Solution

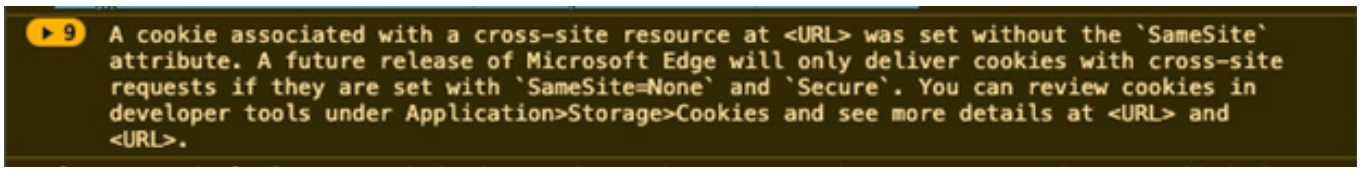
Technical Bulletin:
Google Chrome SameSite cookie changes

At Cardinal, we're always making sure you don't get surprised by outside updates that can impact your authentication flow. Read on to see what you can do to avoid these errors.

What changed and how was I affected?

This past February, Google officially launched version 80 of its Chrome browser in their continued efforts to make the web more secure. The newest version enforces explicit cookie settings, validating that all cookies are not accessible by "third-party" entities by default. This change was rolled out slowly over several weeks, officially reaching the general population of Chrome users by March 9, 2020. As of April 2020, Google has rolled this change back due to complications related to COVID-19. At this time, there is no date for re-enabling this feature, though this will likely occur mid-summer 2020.

If you are using cookies as part of your checkout flow to retain values related to the consumers session, you may be impacted. Depending on how you have chosen to integrate your 3-D Secure solution, you may experience issues with authentication. In extreme cases, you may have trouble fully completing an order.



If you were not previously explicitly setting the SameSite attribute on your cookies, the Chrome 80 update will set this attribute to "Lax" by default. The SameSite attribute requires all cookies to be "first-party," meaning the URL on the browser must match the domain of the cookie.

To note: These updates will impact the most recent versions of Google Chrome, other Chromium-based browsers such as the latest Microsoft Edge for Windows and macOS.

What can be done to remedy the situation?

There are several ways you can ensure your integration is not impacted by this change. Please review the options below to determine the best solution for your needs.

Option #1: Explicitly mark cross-site cookies by implementing the SameSite attribute

On any cookies you are using to maintain session related to your 3-D Secure checkout flow, explicitly set the SameSite attribute. This will ensure the default value of "Lax" is not implemented by the Chrome browser.

Option #2: Provide an alternate mechanism for retaining session on return from third-party sites that does not require cookies

Utilizing Form POSTs or other methods, you may be able to eliminate the need for cookies related to sessioning. Other options include external state management utilizing frameworks such as Redis.

Option #3: Leverage an optional merchant data field available on the Form POST that can be used to help track the customer session

In both 3-D Secure 1.0.2 and EMV® 3-D Secure , there are optional merchant data / session fields available to suit this use case.

In 3DS 1.0.2, you can look to leverage the MD field on the PAReq endpoint.

- *The MD ("Merchant Data") field: merchant state data that must be returned to the merchant.*
- *This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session.*
- *Since the content of this field varies by merchant implementation, the ACS must preserve it unchanged and without assumptions about its content.*

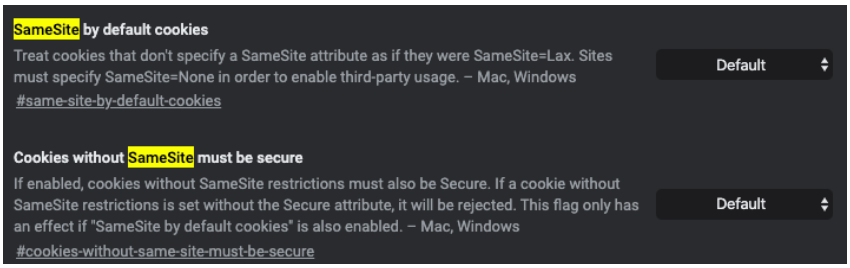
In EMV 3DS (versions 2.1 and 2.2), the threeDSSessionData field is available to facilitate similar interactions.

- *3DS Requestor session data that is returned by the ACS in the CRes message POST to the 3DS Requestor. Optionally used to accommodate the different methods 3DS Requestor systems handle session information.*
- *If the 3DS Requestor system can associate the final post with the original session without further assistance, the 3DS Requestor Session Data field may be missing.*
- *If the 3DS Requestor system does not maintain a session for a given authentication session, the 3DS Requestor Session Data field can carry any data the 3DS Requestor needs to continue the session.*
- *Because the content of this field varies by 3DS Requestor implementation, the ACS preserves the content unchanged and without assumptions.*

How can I test my changes?

"To see how a site or service will behave under the new model, we strongly recommend testing in Chrome 76+ with the "SameSite by default cookies" and "Cookies without SameSite must be secure" experimental flags enabled. (To enable flags to go chrome://flags.) Since the new model will roll out to Chrome 80 gradually, when testing, you should also enable the flags in Chrome 80 to make sure your browser reflects the new default settings.

You can also test whether any unexpected behavior you're experiencing in Chrome 80 is attributable to the new model by disabling the "SameSite by default cookies" and "Cookies without SameSite must be secure" flags. If the issue persists with the flags disabled, then the cookie changes are probably not the cause of the issue." [1]



Additional Information

As we discussed, recent changes made by Google to its Chrome browser and cookie settings may affect you. We have outlined how to solve for possible issues based on your needs, and how to test to make sure that your fix was successful! If you have any questions, let's talk. We're here to help.

Visit cardinalcommerce.com or **call** +1.440.352.8444

You can also reference the sites below for more info on updates and what you need to know.

SameSite Updates -
https://www.chromium.org/updates/same-site

"Fixing issues with SameSite cookies and 3-D Secure checkout flows" -
https://github.com/GoogleChromeLabs/samesite-examples/blob/3d-secure-impl/3d-secure.md

[1] "SameSite Cookie Changes in February 2020: What You Need to Know" -
https://blog.chromium.org/2020/02/samesite-cookie-changes-in-february.html

cardinal
A Visa Solution