

Script Integrity Verification for Payment Pages

Download the PDF of this article.

In this Article

Related Articles

Introduction

If you use custom scripts on a payment page, FormAssembly monitors those scripts for unexpected changes. This feature, called Script Integrity Verification, helps protect your respondents' payment card data by alerting you when a script loaded on your payment page has been modified.

When FormAssembly detects that a script on your payment page has changed, the form owner will receive an email notification. They will then have **5 days** to review the change and verify that the updated script is safe. If the script is not verified within that window, it will be blocked from running on the payment page.

This feature is part of FormAssembly's commitment to PCI DSS compliance and helps safeguard your forms against unauthorized script tampering.

Why This Matters

Payment pages are a common target for malicious actors. One way attackers try to steal payment card information is by injecting or modifying scripts that run on a page where cardholders enter their data. These tampered scripts can silently capture card numbers, expiration dates, and other sensitive information without the form owner's knowledge.

Script Integrity Verification adds a layer of protection by continuously checking that the scripts on your payment pages match the versions you've approved. If anything changes, you'll know about it right away.

How It Works

FormAssembly uses a technique called Subresource Integrity (SRI) to track the contents of external scripts loaded on your payment pages. Here's what to expect:

1. **FormAssembly records a fingerprint of each script** running on your payment page. This fingerprint is based on the script's contents at the time it was last verified.
 2. **If a script's contents change**, FormAssembly detects the mismatch and sends an email notification to the form owner.
 3. **You have 5 days to verify the change.** During this window, the script will continue to function normally on your payment page.
 4. **If the script is not verified within 5 days**, it will be blocked from running on the payment page. This is a protective measure to prevent potentially compromised scripts from accessing cardholder data.
-

What to Do When You Receive a Notification

When you receive a script change notification email, it means that a script loaded on one of your payment pages has been modified since it was last verified. Here's how to respond:

If You Expected the Change

If you or your team recently updated the script, or if the script's provider (such as an analytics or tracking service) released a new version, you can verify the script to confirm that the change is legitimate.

To verify the script, follow the instructions in the notification email and review the script attached to the form. Once verified, FormAssembly will update the stored fingerprint and resume normal monitoring.

If You Did Not Expect the Change

If the change was not anticipated, **do not verify the script**. Instead, take the following steps:

1. **Review the script** that is running on your payment page. Check the script's source and confirm whether it has been altered without your knowledge.
2. **Contact the script provider** if the script is loaded from a third-party service. Ask whether they recently pushed an update.
3. **Remove or replace the script** if you cannot confirm the change is safe.

Note: Even if you choose not to verify the script, it will stop functioning on your payment page after the 5-day window expires. This ensures that unverified scripts cannot continue to run on pages that collect payment information.

Frequently Asked Questions

Which forms does this apply to?

- Script Integrity Verification applies to any form that includes a payment connector, such as Stripe, PayPal, Authorize.Net, CyberSource, or any other supported payment integration. If your form does not collect payment information, this feature does not apply.

What counts as a "script" on my payment page?

- This includes any JavaScript loaded on your payment page through custom code, HTML sections, or external script references. It does not include FormAssembly's own scripts, which are managed and verified separately.

Will my form stop working if I don't verify in time?

- The form itself will continue to function, but the unverified script will be blocked from running. If the script is essential to your form's functionality (for example, a custom validation or calculation), that specific functionality will stop working until the script is verified or replaced.

Can I re-verify a script after it has been blocked?

- Yes. If a script has been blocked because it was not verified within the 5-day window, you can still verify it at any time. Once verified, the script will be allowed to run on your payment page again.

I don't use any custom scripts on my payment page. Will I receive these notifications?

- If you have not added any custom JavaScript or external script references to your payment form, you should not receive these notifications. If you do receive one unexpectedly, contact FormAssembly Support immediately, as it may indicate unauthorized changes to your form.
-