Delivery headers

HTTP POST payloads that are delivered to your webhook's configured URL endpoint will contain several special headers:

Header	Description
X-GitHub-Event	Name of the event that triggered the delivery
X-GitHub-Delivery	A GUID to identify the delivery
X-Hub-Signature	This header is sent if the webhook is configured with a secret. This is the HMAC hex digest of the request body, and is generated using the SHA-1 hash function and the scret as the HMAC key. X-Hub-Signature is provided for compatibility with existing integrations, and we recommend that you use the more secure X-Hub-Signature-256 instead
X-Hub-Signature-256	This header is sent if the webhook is configured with a secret. This is the HMAC hex digest of the request body, and is generated using the SHA-256 hash function and the secret as the HMAC key.

Also, the User-Agent for the requests will have the prefix GitHub-Hookshot.

Example delivery

```
> POST /payload HTTP/2

> Host: localhost:4567
> X-GitHub-Delivery: 72d3162e-cc78-11e3-81ab-4c9367dc0958
> X-Hub-Signature: sha1=7d38cdd689735b008b3c702edd92eea23791c5f6
> X-Hub-Signature-256:
sha256=d57c68ca6f92289e6987922ff26938930f6e66a2d161ef06abdf1859230aa23c
> User-Agent: GitHub-Hookshot/044aadd
> Content-Type: application/json
> Content-Length: 6615
> X-GitHub-Event: issues

> {
>   "action": "opened",
>   "issue": {
>     "url": "https://api.github.com/repos/octocat/Hello-World/issues/1347",
>     "number": 1347,
>     ...
>   },
>   "repository" : {
>     "id": 1296269,
>     "full_name": "octocat/Hello-World",
>     "owner": {
>       "login": "octocat",
>       "id": 1,
>       ...
```

```
>     },
>     ...
>   },
>   "sender": {
>     "login": "octocat",
>     "id": 1,
>     ...
>   }
> }
```

관련 문서

Plugin Backlinks: 아무 것도 없습니다.