Report-To header

- Syntax
- Examples
  - Setting a CSP violation report endpoint
  - Specifying multiple reporting groups
- Specifications
- Browser compatibility
- See also

> **WARNING:** This header has been replaced by the Reporting-Endpoints HTTP response header. It is a deprecated part of an earlier iteration of the Reporting API specification.

The HTTP `Report-To` response header allows website administrators to define named groups of endpoints that can be used as the destination for warning and error reports, such as CSP violation reports, Cross-Origin-Opener-Policy reports, deprecation reports, or other generic violations.

`Report-To` is often used in conjunction with other headers that select a group of endpoints to use for a particular kind of report. For example, the Content-Security-Policy header report-to directive can be used to select the group used for reporting CSP violations.

Header type	[Response header](https://developer.mozilla.org/en-US/docs/Glossary/Response%20header)
[CORS-safelisted response header](https://developer.mozilla.org/en-US/docs/Glossary/CORS-safelisted%20response%20header)	No

Syntax

```
Report-To: <json-field-value>
```

- `<json-field-value>`
  - : One or more endpoint-group definitions, defined as a JSON array that omits the surrounding `[` and `]` markers. Each object in the array has the following members:
    - `group`
      - : A name for the group of endpoints.
    - `max_age`
      - : The time in seconds that the browser should cache the reporting configuration.
    - `endpoints`
      - : An array of one or more URLs where the reports in the group should be sent.

Examples

Setting a CSP violation report endpoint

This example shows how a server might use `Report-To` to define a group of endpoints, and then set the group as the location where CSP violation reports are sent.

First a server might send a response with the `Report-To` HTTP response header as shown below. This specifies a group of `url` endpoints identified by the group name `csp-endpoints`.

```
Report-To: { "group": "csp-endpoints",
             "max_age": 10886400,
             "endpoints": [
               { "url": "https://example.com/reports" },
               { "url": "https://backup.com/reports" }
             ] }
```

The server can then specify that it wants this group to be the target for sending CSP violation reports by setting the group name as the value of the report-to directive:

```
Content-Security-Policy: script-src https://example.com/; report-to csp-endpoints
```

Given the headers above, any `script-src` CSP violations would result in violation reports being sent to both of the `url` values listed in `Report-To`.

Specifying multiple reporting groups

The example below demonstrates a `Report-To` header that specifies multiple endpoint groups. Note that each group has a unique name, and that the groups are not bounded by the array markers.

```
Report-To: { "group": "csp-endpoint-1",
             "max_age": 10886400,
             "endpoints": [
               { "url": "https://example.com/csp-reports" }
             ] },
           { "group": "hpkp-endpoint",
             "max_age": 10886400,
             "endpoints": [
               { "url": "https://example.com/hpkp-reports" }
             ] }
```

We can select an endpoint group as the target for violation reports by name, in the same way as we did in the previous example:

```
Content-Security-Policy: script-src https://example.com/; report-to csp-endpoint-1
```

Specifications

This header is no longer part of any specification. It was previously part of the Reporting API.

Browser compatibility

See also

- Reporting API and Reporting-Endpoints header
- report-to CSP directive
- Content-Security-Policy, Content-Security-Policy-Report-Only headers
- Content Security Policy (CSP) guide

□□□ #3
□ □□□ □□□ 2026-10-31 03:27:53 UTC

 cocobook-sync □□□ 2026-11-04 17:35:59 UTC