INTERNET-DRAFT
Intended Status: Standards Track
Expires: 30 August 2026

R. Bouziane
SecRoot.io
1 March 2026

Enforcement-Action HTTP Header Field
draft-secroot-ooda-http-03

Abstract

This document defines the Enforcement-Action HTTP response header field. The field provides a minimal, interoperable mechanism for signaling advisory enforcement coordination between cooperating components operating within a defined administrative or policy trust boundary. The header conveys a single action token and optional parameters without modifying HTTP status code semantics or representation meaning. The field is designed to be safely ignored by recipients that do not recognize it and to operate over existing HTTP deployments without changes to transport protocols. This specification defines the syntax, semantics, processing rules, and IANA registration for the header field.

1. Introduction

HTTP defines status codes that communicate the outcome of request processing and header fields that control caching and representation semantics.

In certain deployments, including reverse proxies, API gateways, and other cooperating components operating within a shared trust boundary, there are cases where a response must remain semantically successful (e.g., 200 OK) while still signaling an advisory enforcement coordination adjustment.

Existing HTTP status codes describe request outcomes and are not intended to convey advisory enforcement coordination independent of transaction semantics.

This document defines the Enforcement-Action HTTP response header field to provide a minimal signaling mechanism while preserving existing HTTP semantics. This specification does not standardize enforcement algorithms, detection models, token vocabularies, coordination frameworks, or operational enforcement mechanisms.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in BCP 14 (RFC 2119, RFC 8174) when, and only when, they appear in all capitals.

For the purposes of this specification, a trusted boundary is defined as a set of components operating under coordinated administrative or policy control, or under explicit bilateral trust configuration.

3. Problem Statement

HTTP status codes communicate the result of processing a specific request. They are not designed to convey advisory enforcement coordination independent of that result.

In deployments involving intermediaries within a trusted boundary, there are scenarios where enforcement coordination must occur without modifying client-visible semantics.

This document defines a minimal HTTP response header field to support such coordination while preserving HTTP protocol behavior and semantic layering.

4. Header Field Definition

4.1. Field Name

The header field name is:

Enforcement-Action

This field is defined for use in HTTP responses only. The Enforcement-Action field is an end-to-end response header field.

4.2. Syntax

The Enforcement-Action field value is defined using ABNF (RFC 5234):

```
Enforcement-Action = action-token *( OWS ";" OWS parameter )

action-token       = token
parameter          = token "=" token
```

The definitions of "token" and "OWS" are imported from RFC 9110.

4.3. Semantics

The Enforcement-Action header field conveys an advisory, deployment-defined enforcement coordination signal associated with the response.

The presence of the field does not modify HTTP status code semantics, representation metadata, caching semantics, or content negotiation behavior.

This specification does not define specific action tokens. The meaning of action tokens and parameters is deployment-defined.

5. Processing Rules

5.1. General

The Enforcement-Action header field is defined for HTTP responses only. Recipients MUST ignore the field if received in an HTTP request.

The field MUST NOT be included in 304 (Not Modified) responses.

5.2. Sender Behavior

A sender MAY include the Enforcement-Action header field in a response to convey an advisory enforcement coordination signal.

Senders SHOULD generate the field only within authenticated or policy-trusted contexts operating within a trusted boundary.

A sender MUST NOT rely on recipients to enforce a specific action.

5.3. Recipient Behavior

Recipients MAY ignore the Enforcement-Action field entirely.

Recipients MUST NOT assume authenticity or integrity beyond what is provided by the underlying transport security.

Recipients MUST only honor the Enforcement-Action field when it is received from authenticated and policy-trusted sources operating within a defined trusted boundary.

Recipients that recognize the field:

* MUST parse the field according to Section 4.
* MUST treat unrecognized action tokens as no-op.
* MUST ignore unrecognized parameters.
* MUST ignore the entire field if parsing fails.
* MUST NOT alter HTTP status semantics based solely on the field.

5.4. Multiple Header Instances

A response SHOULD include at most one Enforcement-Action header field.

If multiple instances are present, recipients MUST process only the first occurrence and ignore subsequent instances.

6. Intermediary Behavior

Intermediaries MAY forward the Enforcement-Action header field unchanged.

Intermediaries operating within a trusted boundary MAY consume and

remove the header before forwarding the response beyond that boundary.

Intermediaries SHOULD remove the header when forwarding responses beyond the intended trusted boundary unless explicitly configured otherwise.

Intermediaries MUST NOT modify HTTP status code semantics solely due to the presence of the Enforcement-Action field.

7. Caching Considerations

The presence of the Enforcement-Action header field does not modify HTTP caching semantics.

Caches MUST evaluate cacheability according to existing HTTP caching rules independent of the presence of this field (RFC 9111).

Deployments that use Enforcement-Action for client-specific coordination SHOULD ensure that responses containing the field are not reused across unrelated clients unless explicitly intended.

8. Security Considerations

The Enforcement-Action header field conveys advisory enforcement coordination signals. Improper interpretation may result in unintended policy decisions within a deployment.

The field does not provide authentication, authorization, integrity, or confidentiality guarantees beyond those provided by the underlying HTTP transport.

When used over authenticated transports (e.g., HTTPS), the field benefits from transport security. When used over unauthenticated transports, it may be modified or injected by on-path attackers.

Recipients MUST treat the field as untrusted unless received from authenticated and policy-trusted sources operating within a defined trusted boundary.

Intermediaries and recipients SHOULD consider the potential disclosure of operational enforcement posture when forwarding the field beyond a trusted boundary.

The field MUST NOT be interpreted as a replacement for HTTP authentication, authorization, rate-limiting, or access control mechanisms.

9. IANA Considerations

IANA is requested to register the following HTTP response header field in the "Hypertext Transfer Protocol (HTTP) Field Name Registry":

Field Name:	Enforcement-Action
Status:	permanent
Reference:	This document

No additional IANA registries are created by this specification.

10. Examples

The following examples illustrate possible uses of the Enforcement-Action header field. These examples are deployment-specific and are provided for illustrative purposes only.

Example 1:

```
HTTP/1.1 200 OK
Content-Type: application/json
Enforcement-Action: isolate
```

Example 2:

```
HTTP/1.1 200 OK
Content-Type: text/html
Enforcement-Action: throttle; score=87
```

11. Non-Goals

This specification does not:

* Define a threat model or attack taxonomy.
* Define enforcement algorithms or decision logic.
* Standardize action token vocabularies or parameter registries.
* Establish a control-plane coordination protocol.
* Replace HTTP authentication, authorization, or access control mechanisms.
* Modify HTTP status code semantics or transaction outcome behavior.

The Enforcement-Action header field defines only a minimal advisory signaling surface within a trusted boundary.

Appendix A. Change History

This header field was previously named "OODA-Action". It has been renamed to "Enforcement-Action" to reflect the narrowed, framework-neutral scope of this specification.

12. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174.

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications", RFC 5234.

[RFC9110] Fielding, R., Ed., "HTTP Semantics", RFC 9110.

[RFC9111] Fielding, R., Ed., "HTTP Caching", RFC 9111.

Author’s Address

Rachid Bouziane
SecRoot.io
Email: contact@secroot.io
Morocco