NAME

httpstatus — HTTP status codes

DESCRIPTION

This manual page documents the HTTP status codes commonly issued by a web server in response to a client request. The status codes in this manual page are based on the information found in RFC7231 unless otherwise noted.

HTTP status codes fall into one of five classes, identified by the first digit as follows:

1xx (Informational)
: The request was received, continuing process.

2xx (Successful)
: The request was successfully received, understood, and accepted.

3xx (Redirection)
: Further action needs to be taken in order to complete the request.

4xx (Client Error)
: The request contains bad syntax or cannot be fulfilled.

5xx (Server Error)
: The server failed to fulfill an apparently valid request.

1xx STATUS CODES

100 Continue
: The server has received the initial part of the request and the client should proceed to send the remainder.

101 Switching Protocols
: The server agrees to the client's request to switch protocols via the RFC7230 "Upgrade" header.

102 Processing
: The server has has accepted the complete request, but has not yet completed it. (WebDAV; RFC2518)

103 Early Hints
: The server is likely to send a final response with the header fields included in the informational response. (RFC8297)

2xx STATUS CODES

200 Ok
: The request has succeeded.

201 Created
: The request has been fulfilled and has resulted in one or more new resources being created.

202 Accepted
: The request has been accepted for processing, but the processing has not been completed.

203 Non-Authoritative Information
: The request was successful but the enclosed payload has been modified from that of the origin server's 200 (OK) response by a transforming proxy.

204 No Content
: The server has successfully fulfilled the request; there is no additional content to send in the response payload body.

205 Reset Content
The server has fulfilled the request; the client should reset its document view.

206 Partial Content
The server is successfully fulfilling a range request for the target resource based on the client's "Range" header. (RFC7233)

207 Multi-Status
Multiple resources were to be affected by the COPY, but errors on some of them prevented the operation from taking place. (WebDAV; RFC4918)

208 Already Reported
Indicates that members of multiple bindings from a previous multi-status response are not repeated. (WebDAV; RFC5842)

226 IM Used
The server has fulfilled a GET request for the resource, and the response is a representation of the result of one or more instance- manipulations applied to the current instance. (RFC3229)

3xx STATUS CODES

300 Multiple Choices
The target resource has more than one representation which the client may choose from via Content Negotiation.

301 Moved Permanently
The target resource has been assigned a new permanent URI and any future references to this resource ought to use one of the enclosed URIs.

302 Found
The target resource resides temporarily under a different URI.

303 See Other
The server is redirecting the user agent to a different resource, as indicated by a URI in the Location header field.

304 Not Modified
A conditional GET or HEAD request has been received and would have resulted in a 200 (OK) response if it were not for the fact that the condition evaluated to false. (RFC7232)

305 Use Proxy
The requested resource MUST be accessed through the proxy given by the Location field. (RFC2616) Deprecated due to security concerns regarding in-band configuration of a proxy.

306 Switch Proxy
No longer used. Originally generated by a proxy server to indicate that the client or proxy should use the information in the accompanying 'Set- proxy' header to choose a proxy for subsequent requests.

307 Temporary Redirect
The target resource resides temporarily under a different URI and the user agent MUST NOT change the request method if it performs an automatic redirection to that URI.

308 Permanent Redirect
The target resource has been assigned a new permanent URI and any future references to this resource ought to use one of the enclosed URIs. (RFC7538)

4xx STATUS CODES

400 Bad Request
The server cannot or will not process the request due to something that is perceived to be a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

401 Unauthorized
The request has not been applied because it lacks valid authentication credentials for the target resource.

402 Payment Required
Reserved for future use.

403 Forbidden
The server understood the request but refuses to authorize it.

404 Not Found
The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

405 Method Not Allowed
The method received in the request-line is known by the origin server but not supported by the target resource.

406 Not Acceptable
The target resource does not have a current representation that would be acceptable to the user agent, such as due to the client's "Accept" header.

407 Proxy Authentication Required
The client needs to authenticate itself in order to use a proxy. (RFC7235)

408 Request Timeout
The server did not receive a complete request message within the time that it was prepared to wait.

409 Conflict
The request could not be completed due to a conflict with the current state of the target resource.

410 Gone
Access to the target resource is no longer available at the origin server; this condition is likely to be permanent.

411 Length Required
The server refuses to accept the request without a defined Content-Length.

412 Precondition Failed
One or more conditions given in the request header fields evaluated to false when tested on the server. (RFC7232)

413 Payload Too Large
The server is refusing to process a request because the request payload is larger than the server is willing or able to process.

414 URI Too Long
The server is refusing to service the request because the request-target is longer than the server is willing to interpret.

415 Unsupported Media Type
The origin server is refusing to service the request because the payload is in a format not supported by this method on the target resource.

416 Range Not Satisfiable
None of the ranges in the request's Range header field overlap the current extent of the selected resource or the set of ranges requested has been rejected due to invalid ranges or an excessive request of small or overlapping ranges. (RFC7233)

417 Expectation Failed
The expectation given in the request's Expect header field could not be met by at least one of the inbound servers.

418 I'm a teapot
An attempt to brew coffee was made, even though the target is a teapot. (RFC2324)

421 Misdirected Request
The request was directed at a server that is not able to produce a response. (RFC7540)

422 Unprocessable Entity
The server understands the content type of the request entity and the syntax of the request entity is correct, but was unable to process the contained instructions. (WebDAV; RFC4918)

423 Locked
The source or destination resource of a method is locked. (WebDAV; RFC4918)

424 Failed Dependency
The method could not be performed on the resource because the requested action depended on another action and that action failed. (WebDAV; RFC4918)

425 Too Early
The server is unwilling to risk processing a request that might be replayed. (RFC8470)

426 Upgrade Required
The server refuses to perform the request using the current protocol but might be willing to do so after the client upgrades to a different protocol.

428 Precondition Required
The origin server requires the request to be conditional. (RFC6585)

429 Too Many Requests
The user has sent too many requests in a given amount of time. (RFC6585)

431 Request Header Fields Too Large
The server is unwilling to process the request because its header fields are too large. (RFC6585)

451 Unavailable For Legal Reasons
The server is denying access to the resource as a consequence of a legal demand. (RFC7725) Named after Ray Bradbury's "Fahrenheit 451".

5xx STATUS CODES

500 Internal Server Error
The server encountered an unexpected condition that prevented it from fulfilling the request.

501 Not Implemented
The server does not support the functionality required to fulfill the request.

502 Bad Gateway
The server, while acting as a gateway or proxy, received an invalid response from an inbound server it accessed while attempting to fulfill the request.

503 Service Unavailable
The server is currently unable to handle the request due to a temporary overload or scheduled maintenance, which will likely be alleviated after some delay.

504 Gateway Timeout
The server, while acting as a gateway or proxy, did not receive a timely response from an upstream server it needed to access in order to complete the request.

505 HTTP Version Not Supported
The server does not support, or refuses to support, the major version of HTTP that was used in the request message.

506 Variant Also Negotiates
The server's chosen variant resource is configured to engage in transparent content negotiation itself, and is therefore not a proper end point in the negotiation process. (RFC2295)

507 Insufficient Storage
The method could not be performed on the resource because the server is unable to store the representation needed to successfully complete the request. (WebDAV; RFC4918)

508 Loop Detected
The server terminated an operation because it encountered an infinite loop while processing a request with "Depth: infinity". (WebDAV; RFC5842)

510 Not Extended
The policy for accessing the resource has not been met in the request. (RFC2774)

511 Network Authentication Required
The client needs to authenticate to gain network access. (RFC6585)

NON STANDARD HTTP STATUS CODES

In addition to the above, several HTTP server or proxy implementations include custom status codes, particularly in the 4xx and 5xx classes.

000 (AWS ELB)
Used by AWS Elastic Load Balancing with HTTP/2 GOAWAY frame if the compressed length of any of the headers exceeds 8K bytes or if more than 10K requests are served through one connection exceeds 10,000.

000 (curl)
Used by `curl`(1) to indicate a failed execution.

000 Client-Side Abort (Akamai LDS)
Used by Akamai Log Delivery Services if a download was terminated by the end-user before the edge server is able to send back the response header.

000 (Looker Studio)
No HTTP code was received.

218 This is fine (Apache httpd)
A catch-all error condition displayed instead of a 4xx or 5xx error, allowing the passage of message bodies through the server when the `ProxyErrorOverride` setting is enabled.

299 Deprecated (Linode)
The request was successful, but involved a deprecated endpoint.

419 Page Expired (Laravel)
A CSRF Token is missing, expired, or cannot be verified.

430 Shopify Security Rejection (Shopify)
The request was deemed malicious.

440 Login Time-out (Microsoft IIS)
The client's session has expired and must log in again.

444 No Response (nginx)
Used by the ngx_http_rewrite_module to instruct the server to close the connection without sending a response header.

449 Retry With Status Code (Microsoft IIS)
The request cannot be satisfied because insufficient information was provided by the client.

450 Blocked by Windows Parental Controls (Microsoft)
Windows Parental Controls are turned on and are blocking access to the requested webpage.

451 Redirect (Microsoft Exchange)
Used by Microsoft Exchange ActiveSync to indicate that the client is attempting to connect to the wrong server, or if there is a more efficient server to use to reach the user's mailbox

460 (AWS ELB)
The client closed the connection with the load balancer before the idle timeout period elapsed.

462 Not Allowed (Fastly)
The client's IP was blocked.

463 (AWS ELB)
The load balancer received an X-Forwarded-For request header with too many IP addresses.

464 (AWS ELB)
Incompatible protocol versions between the client and the origin server.

492 User Access Forbidden (Akamai EAA)
The client is not authorized to access the application.

493 Unsupported Browser (Akamai EAA)
The client did not send a Server Name Identification (SNI) in the TLS handshake.

494 Request Header Too Large (nginx)
The client sent too large a request or too long a header line.

494 Request Header Or Cookie Too Large (Akamai EAA)
An HTTP Request Header is bigger than the configured buffer value.

498 Invalid Token (Esri)
Used by the Esri ArcGIS Server to indicate an expired or otherwise invalid token.

495 SSL Certificate Error (nginx)
The client has provided an invalid client certificate.

496 496 SSL Certificate Required (nginx)
A client certificate is required but was not provided.

497 HTTP Request Sent to HTTPS Port (nginx)
The client has made an HTTP request to an HTTPS port.

499 Client Closed Request (nginx)
The client has closed the request before the server could send a response.

499 Token Required (Esri)
Used by the Esri ArcGIS Server to indicate that a token is required but was not submitted.

503 Loop Detected (Fastly)
A request appears to originate from the same Fastly service that it is trying to invoke, or the request has transited too many Fastly servers.

509 Bandwidth Limit Exceeded (Apache httpd / cPanel)
The server has exceeded the bandwidth specified by the server administrator.

520 Web Server Returned an Unknown Error (Cloudflare)
The origin server returned an empty, unknown, or unexpected response to Cloudflare.

521 Web Server Is Down (Cloudflare)
The origin server refused connections.

522 Connection Timed Out (Cloudflare)
Time out when contacting the origin server.

523 Origin Is Unreachable (Cloudflare)
The origin server was unreachable.

524 A Timeout Occurred (Cloudflare)
After a successful TCP connection to the origin server the HTTP response timed out.

525 SSL Handshake Failed (Cloudflare)
TLS handshake failure with the origin server.

526 Invalid SSL Certificate (Cloudflare / Cloud Foundry)
Unable to validate the origin server's TLS certificate.

527 Railgun Error (Cloudflare)
Connection interrupted between Cloudflare and the origin server's Railgun server.

529 Site is overloaded (Qualys SSLabs)
API service is overloaded.

530 Internal Edgio Error (Edgio)
An unexpected error.

530 (Cloudflare)
Used by Cloudflare as a generic error status code. More details can be found in the accompanying HTML body describing a 1XXX error code.

530 Site is frozen (Pantheon)
A site that has been frozen due to inactivity.

530 Origin DNS Error (Shopify)
Cloudflare can't resolve the requested DNS record.

531 Project Upstream Connection Error (Edgio)
Unable to establish a connection to the origin server.

532 Project Response Too Large (Edgio)
A returned a response size was greater than the allowed maximum.

533 Project Upstream TLS Error (Edgio)
Unable to establish a TLS connection to the origin.

534 Project Error (Edgio)
The projectâs serverless code has failed unexpectedly or has issued a malformed response.

535 Unknown Project (Edgio)
Missing or mismatching Host header.

536 Project HTTP Response Timeout (Edgio)
Time out when contacting the origin server.

537 Project DNS Resolution Error (Edgio)
The proxy was unable to resolve the host name.

538 Project Request Loop (Edgio)
The request went through too many Edgio servers.

539 Project Timeout (Edgio)
The project's serverless code did not respond in time.

540 Temporarily Disabled (Shopify)
The requested endpoint has been temporarily disabled.

540 Connectivity Disrupted (Akamai EAA)
The connector does not have dial-out connections to either the data POP for the application or access to the directory.

540 Out of Memory (Edgio)
The project's serverless code caused an out-of-memory situation.

541 Edgio Out of Workers (Edgio)
Traffic was too high to be scheduled for processing within the scheduling timeout.

542 Internal Database Error (Akamai EAA)
The data POP cannot reach the authentication database.

542 Project Header Overflow (Edgio)
The project's request or response had too many HTTP headers.

543 IdP Communication Error (Akamai EAA)
The data POP cannot reach the IdP or directory service.

543 Global Upstream Timeout (Edgio)
The request failed to propagate between Edgio edge and the global POP.

544 Management Communication Error (Akamai EAA)
The Login/Authentication POP cannot reach the management login manager.

544 Invalid Host Header (Edgio)
The Host header is not a valid domain name.

545 Authentication Internal Error (Akamai EAA)
The data POP cannot resolve/reach the authentication database.

545 Edgio Component Not Ready (Edgio)
An unprepared Edgio component received traffic.

546 Unknown Application (Akamai EAA)
The Login/Authentication POP does not have the application configuration.

546 Edgio Global POP TLS Error (Edgio)
An error occurred negotiating a secure TLS connection with the Edgio global POP.

547 Edgio Global POP No HTTP Response (Edgio)
No HTTP response from the global POP.

548 Invalid Response (Akamai EAA)
The response received from the login server could not be validated via back-channel request from the cloud proxy to the login server.

548 Edgio Global POP DNS Resolution Error (Edgio)
Failure to resolve the global POP's host name through the DNS.

549 Authentication Gateway Error (Akamai EAA)
The Login service cannot reach directories to complete the authentication process.

552 Application Unreachable (Akamai EAA)
The application service is not reachable from connector.

553 Directory Service Error (Akamai EAA)
A directory service error during Kerberos authentication.

554 Authentication Token Error (Akamai EAA)
The Kerberos token is not accepted by application.

555 Application does not support Kerberos (Akamai EAA)
No negotiate option found in 401 challenge.

556 Unexpected Authentication Challenge (Akamai EAA)
Encountered a 401 challenge on a URI not configured as login URI.

557 KDC Unreachable (Akamai EAA)
The KDC is unreachable.

558 Connection Limit Stop: Service Concurrent Connections Exceeded (Akamai EAA)
A user has established too many WebSocket connections.

559 Connection Limit Stop: Service Concurrent Connections Exceeded (Akamai EAA)
A user has established too many WebSocket connections.

561 Invalid NTLM Challenge (Akamai EAA)
The connector received an invalid NTLM challenge from server.

561 Unauthorized (AWS ELB)
IdP could not authenticate the user.

562 Credential Error (Akamai EAA)
Unable to encrypt or decrypt NTLM credentials.

598 Network Read Timeout Error
Used by some HTTP proxies to signal a network read timeout behind the proxy to a client in front of the proxy.

599 Network Connect Timeout Error
Used by some HTTP proxies to signal a network connect timeout behind the proxy to a client in front of the proxy.

600 (Akamai)
Used by Akamai to indicate various invalid headers.

783 Unexpected Token (Shopify)
The request includes a JSON syntax error.

893 (Edgio)
Used by Edgio when load balancing high volume traffic for a specific asset within a POP.

SEE ALSO

RFC2324, RFC2518, RFC2616, RFC3229, RFC4918, RFC5842, RFC6585, RFC7230, RFC7231, RFC7232, RFC7233, RFC7538, RFC7540

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

HISTORY

This list of HTTP status codes was originally compiled into a manual page by Jan Schaumann ⟨jschauma@netmeister.org⟩ in July 2021.