5XX SERVER ERROR CODES

Error codes in the 5xx range indicate server problems. The descriptions for most codes are self-explanatory. following sections.

500 -Internal Server Error
501 -Not Implemented
502 -Bad Gateway
503 -Service Unavailable

HTTP 500.*x* — Internal Server Error Codes

The most common 500 Substatus Codes returned by IIS are listed below. The descriptions for most substatus codes are self-explanatory.

500	none	Internal Server Error
	11	Application is shutting down on the Web server.
	12	Application restarting
	13	Server too busy
	14	Invalid application configuration on the server.
	15	Direct requests for GLOBAL.ASA forbidden
	16	UNC authorization credentials are incorrect.
	17	URL authorization store not found
	18	URL authorization store cannot be opened
	19	Bad file metadata
	100	ASP error

503-Service Unavailable

HTTP 503 errors are returned more often in IIS 6.0 than in earlier versions of IIS. Typically, the HTTP 503-Service Unavailable error is returned directly from HTTP.sys when there is a problem with getting the request up to the worker process. However, this error can occur for a variety of reasons, as listed.

For security purposes, the description that is sent back to the client (Service Unavailable) does not fully describe the error. HTTP.sys keeps its own error log. Requests that generate 503 errors never pass into user mode; therefore, the HTTP error log is the only place these problems are documented. To troubleshoot the cause of the 503 error, use the following procedure.

Reason String	Text in HTTP.sys Error Log	Cause(s) of Error
Service unavailable.	N/A	IIS cannot start any new worker processes because of limited system resources or because starting a new worker process would exceed the **DemandStartThreshold** property. Bandwidth throttling is enabled, but the filter addition fails. The control channel or internal configuration group for the URL is inactive. The send for a request that was serviced from the cache failed (typically under low memory conditions).
Too many users.	ConnLimit	The connection limit for the site or server as a whole has been reached.
Application taken offline.	AppOffline	The application pool has been put into Rapid Fail Protection and has been disabled automatically.
Application request queue full.	QueueFull	The application pool's request queue has been exceeded and the request cannot be queued.
Administrator has taken application offline.	Disabled	The administrator has stopped the application pool.
Application automatically shut down due to administrator policy.	AppShutdown	The application pool has been shut down because it exceeded its CPU usage limit.
Request timed out in app pool queue.	AppPoolTimer	The application pool is too busy to handle the request. The request has, therefore, timed out in the queue and has been returned with a 503 error.

Microsoft

IIS 6.0 HTTP Status Codes Cribsheet

HTTP 1XX-2XX — INFORMATIONAL & SUCCESS

HTTP status codes in the 1xx are typically informational. Status codes in the 2xx range indicate that the transaction was successful. The codes in both ranges are self-explanatory.

HTTP 3XX — REDIRECTION CODES

HTTP status codes in the 3xx range pertain to redirection (telling the browser to issue a new request at a different location). These codes do not indicate that a problem has occurred.

301-Permanent Redirect

This redirection status code tells the Web client that the location for the requested resource has permanently changed. The new location is specified in the Location HTTP header. This is primarily useful for Web clients that keep record of HTTP URL links. Upon receiving this status code, the Web client can update the stored URL with the new location.

302-Object Moved

This standard redirection status code tells the Web client to issue a new request to the location specified in the Location HTTP header.

304-Not Modified

RFC 2616, Hypertext Transfer Protocol — HTTP/1.1 provides functionality for "conditional GET requests." For example, an HTTP client can specify an If-Modified-Since HTTP header that consists of a time and date stamp, which tells the server that it has a cached copy of the content being requested. If the request meets the condition specified in the If-Modified-Since header, the server will not return a body, but will return the 304-Not Modified result.

307-Temporary Redirect

The temporary redirect option is used to prevent a Web browser from losing data when the browser issues an HTTP POST request. Normally, when a Web browser issues a POST request and then receives a 302-Object Moved redirect message from the Web server, the browser issues a GET request for the new location and loses the data in the POST request. With a 307 redirect, the browser reissues the POST request with the original data to the new location.

Courtesy Redirects

When a browser makes an HTTP request, the request sometimes takes the form http://example.contoso.com/vdir1. Notice that there is no trailing "/" at the end of the URL. In this case, vdir1 is a directory, instead of a file. As a courtesy to the Web browser, IIS responds to this request with a 302-Object Moved redirect message with the HTTP header: Location: /vdir1/. This is known as a courtesy redirect.

HTTP 40X — CLIENT ERROR CODES

HTTP status codes in the 4xx range indicate that a problem occurred with the request. Request problems can range from the request not meeting authentication requirements to the request being malformed. RFC 2616, Hypertext Transfer Protocol —

HTTP/1.1 refers to request problems as client errors because the requests originate from the client.

HTTP 400-Cannot Resolve the Request

IIS returns a 400 error code when the request is malformed. Though there are a variety causes for this error, the most common reason is that the request does not comply with RFC 2616. HTTP.sys records some errors in its own log file. HTTP.sys Logged Reason Codes for HTTP 400 Errors lists the HTTP.sys reason codes and explanations for each of the 400 errors. These errors are not recorded in the IIS logs.

Reason Code	Condition
BadRequest	The request could not be understood by the server because the syntax was incorrect.
Verb	Invalid verb.
URL	Invalid URL.
Header	Invalid header name.
Hostname	Invalid hostname.
Invalid_CR/LF	Invalid carriage return or line feed.
Number	Invalid number.
FieldLength	A header field in the request was too long.
RequestLength	The request length was too long.

HTTP 401.x-Unauthorized

Authentication is one of the first operations performed when an HTTP request is issued. Authentication is the process whereby IIS creates a user context for an HTTP request, typically by obtaining credentials from the HTTP client using a preconfigured authentication method, and then calling a Windows logon API using those credentials. After the authentication process concludes, IIS determines where the HTTP request goes next based on the resource that is being requested. Regardless of this choice, IIS issues an authorization check against the requested resource. IIS checks to ensure that the user context associated with this request is allowed to make the request. Usually, IIS performs a file ACL check to authenticate the request.

401	1	Unauthorized – Logon failed Access is denied due to invalid credentials.
	2	Access is denied due to server configuration favoring an alternate authentication method
	3	Access is denied due to an ACL set on the requested resource.
	4	Authorization failed by a filter installed on the Web server.
	5	Authorization failed by an ISAPI/CGI application.
	7	Access denied by URL authorization policy on the Web server.

When IIS cannot authenticate a request, it returns a 401.x-Unauthorized code. The substatus codes provide detailed information about why the request failed, as shown previously.

HTTP 403.x-Forbidden

Typically, 403 errors occur when an operation or request is disallowed because a requirement other than proper authentication credentials is not met. Commonly, this error occurs when a script request is made to a Web directory for which script access is not enabled. In such a case, first verify for which resource the request is being made. If the request is, indeed, for script code, such as ASP or ASP.NET, check the execute permissions for that directory in IIS Manager and ensure that at least Script is selected.

403	1	Forbidden – Execute access denied
	2	Read access denied
	3	Write access denied
	4	SSL required
	5	SSL 128 required
	6	IP address rejected
	7	Client certificate required
	8	Site access denied
	9	Too many users
	10	Invalid configuration
	11	Password change
	12	Mapper access denied
	13	Client certificate revoked
	14	Directory listing denied
	15	Client Access Licenses exceeded
	16	Client certificate untrusted or ill-formed
	17	Client certificate has expired or is not yet valid
	18	Cannot execute request from this application pool
	19	CGI access denied
	20	Passport login failed

HTTP 404.x-File or Directory Not Found

A HTTP 404 error indicates that the requested resource was not found. Table 11.8 HTTP 404 Substatus Codes lists the substatus codes for the 404 error. The descriptions for most substatus codes are self-explanatory.

404	none	Not Found
	2	Not Found – Denied due to Lockdown Policy
	3	Not Found – Denied due to MIMEMAP Policy

405-HTTP Verb Used to Access This Page Is Not Allowed

This HTTP code is returned when the client makes an HTTP request that contains a verb that is not allowed. This condition can occur when:

A request for static content contains verbs other than GET or HEAD, and the request is made to a URL that did not end with a "/". Instead performing a courtesy redirect, IIS sends the 405 error.

An HTTP request for an ISAPI application contains a verb not listed in the ScriptMaps configuration for that ISAPI.

407-Initial Proxy Authentication Required by the Web Server

This error indicates that an intermediary proxy server between the HTTP client and the Web server requires some form of authentication. How you troubleshoot this kind of error depends upon the proxy server itself. Generally speaking, running a network trace with Network Monitor is helpful. If the Web client is a custom client, ask its developer to ensure that it is handling security appropriately.

413-Request Entity Is Too Large

For security reasons, you can limit the size of the entity-body of an HTTP request by modifying the MaxRequestEntityAllowed metabase property. When an entity-body of a client request exceeds the size that is specified in the MaxRequestEntityAllowed property, IIS returns a 413 error. If this error is logged for an individual request, an application on the Web server might have encountered an unexpected event and generated a request that is too large. If this error is logged for many requests, a malicious user might be attempting to compromise your Web server.

414-Request URL Is Too Large and Therefore Unacceptable on the Web Server

Just as the entity body of a request can be too large for IIS to process, a URL can be too long for IIS to process. IIS returns a 414 error if this occurs.