Field	Appears As	Description	Default Y/N
Cookie	cs(Cookie)	The content of the cookie sent or received, if any.	N
Referrer	cs(Referrer)	The site that the user last visited. This site provided a link to the current site.	N
Protocol Substatus	sc-substatus	The substatus error code.	Y

Note
FTP log files do not record the following fields:

- cs-uri-query
- cs-host
- cs(User-Agent)
- cs(Cookie)
- cs(Referrer)
- sc-substatus

Multiple W3C Extended log file fields can be selected. However, not all fields will contain information. For fields that are selected but for which there is no information, a hyphen (-) appears as a placeholder. If a field contains a nonprintable character, HTTP.sys replaces it with a plus sign (+) to preserve the log file format. Fields are separated by spaces. Field prefixes have the following meanings:

- s - Server actions
- c - Client actions
- cs - Client-to-server actions
- sc - Server-to-client actions

Note
For the time-taken field, the client-request timestamp is initialized when HTTP.sys receives the first byte, but before HTTP.sys begins parsing the request. The client-request timestamp is stopped when the last IIS send completion occurs. Time taken does not reflect time across the network. The first request to the site shows a slightly longer time taken than other similar requests because HTTP.sys opens the log file with the first request.

HTTP.SYS REASON PHRASES (IIS 6.0)

The following reason phrases can appear in an HTTP.sys error log file to describe the error that caused the log file entry:

Connection_Abandoned_By_AppPool - This reason phrase indicates that the error was caused by a worker process stopping unexpectedly and orphaning requests.

Connection_Dropped - This reason phrase indicates that a zombie connection was dropped by IIS and not resolved correctly.

Various connection time-out errors - These reason phrases include the following various connection time-out errors:

- Timer_ConnectionIdle. There has been no new data sent over the connection since the last send from the client to server, and the connection timed out.
- Timer_HeaderWait. A connection was initiated with the server, but the headers for the request were not received in a timely manner.
- Timer_MinBytesPerSecond. The minimum throughput rate was not maintained.
- Timer_EntityBody. The connection expired while waiting for the entity body to arrive.
- Timer_AppPool. The connection expired because the request waited too long in an application pool queue.

Various errors - These reason phrases include the following errors, most of which are parse errors:

- BadRequest
- Verb
- URL
- Header
- Hostname
- Invalid_CR/LF
- Number
- FieldLength
- RequestLength
- Forbidden
- LengthRequired
- Precondition
- EntityTooLarge
- URL_Length
- Internal
- N/I

Internal - This reason phrase indicates that an HTTP Error 500, internal server error, occurred.

N/I - This reason phrase indicates that an HTTP Error 501, not implemented, occurred.

All 503 errors - The 503 errors are service unavailable errors. These reason phrases include the following 503 errors:

- N/A. The service is unavailable.
- ConnLimit. The site connection limit has been reached.
- AppOffline. Because of rapid fail protection, the application was taken offline by IIS.
- QueueFull. The application request queue is full.
- Disabled. The administrator has taken the application offline.
- AppShutdown. The application was automatically shut down because of an administrator policy.
- AppPoolTimer. The application pool process is too busy to handle the request.

Version_N/S - This reason phrase indicates that an HTTP error 505, HTTP version not supported, occurred.

Microsoft

IIS 6.0 Error Log Cribsheet

LOG FILE FORMATS IN IIS

The following six log file formats are available in IIS:

1. **W3C Extended log file format.** Text-based, customizable format for a single site. This is the default format.
2. **National Center for Supercomputing Applications (NCSA) Common log file format.** Text-based, fixed format for a single site.
3. **IIS log file format.** Text-based, fixed format for a single site.
4. **ODBC logging.** Fixed format for a single site. Data is recorded in an ODBC-compliant database.
5. **Centralized binary logging.** Binary-based, unformatted data that is not customizable. Data is recorded from multiple Web sites and sent to a single log file. To interpret the data, you need a special parser.
6. **HTTP.sys error logging.** Fixed format for HTTP.sys-generated errors.

LOG FILE LOCATIONS AND ACLS

If you create a log file directory of D:\LogFiles for HTTP.sys-generated logging (W3C Extended log file format, NCSA Common log file format, IIS log file format, centralized binary logging, or HTTP.sys error logging), then HTTP.sys generates the following subdirectories, and the log files are created under these subdirectories:

- For the W3C Extended, NCSA Common, and IIS log file formats, HTTP.sys generates the subdirectory

  D:\LogFiles\W3SVC#

  where # is the site ID.
- For centralized binary logging, HTTP.sys generates the subdirectory

  D:\LogFiles\W3SVC

- For HTTP.sys error logging, HTTP.sys generates the subdirectory:

  systemroot\System32\LogFiles\HTTPERR.

By default, the log file directory has the following access control lists (ACLs):

- NT Authority\System: Full access
- Built-in\Administrators: Full access
- Everyone: No access (Although the No access permission is the effective permission, this setting is not explicitly set by HTTP.sys.)

Individual log files in the log file directory have the following controls:

- NT Authority\System: Full access
- Built-in\Administrators: Read and delete access
- Everyone: No access

Important
The default log file directory ACLs (DACLs) are set for optimum security. If log file directories with less restrictive ACLs are created, the system might be more vulnerable to attack.

LOG FILE FORMAT FOR HTTP.SYS ERROR LOGGING

Field	Description
Date	The date, in UTC time. This entry is always 10 characters long, for example, 2000-01-31.
Time	The time, in UTC time. This entry is always eight characters long, for example, 00:12:23.
Client IP	The IP address of the client. The version of the IP address can be either IPv4 or IPv6.
Client Port	The port number of the client.
Server IP	The IP address of the server. The server IP address can be either IPv4 or IPv6.
Server Port	The port number of the server.
Protocol version	The protocol version, if the last request on the connection has been parsed enough to identify the protocol version. If either the major or the minor version is greater than or equal to 10, the driver records the version as "HTTP/?.?".
Verb	The verb, if the last request that was parsed passed the verb state. Unknown verbs are also recorded. HTTP.sys enforces a length limit of 255 bytes for the verb; anything longer is truncated.
CookedURL and query	The URL and its query, if both exist. A question mark (?) separates the URL from the query. If the URL of the request is completely processed (also known as *cooked*), then the processed URL is recorded with a local code page conversion and is treated as a Unicode field. If only the unprocessed (raw) URL was present at the time of logging, then it is recorded as is, without a local code page conversion. HTTP.sys enforces a length limit of 4096 bytes for the URL; anything longer is truncated.
Protocol status	The protocol status of the response for the request, if it is available. The value cannot be greater than 999.
Site ID	The site ID, as a numeric value. For example, instead of recording W3SVC1, the field contains "1." There is no maximum value for the site ID. (This value can be as large as a MAX_ULONG.)
Reason phrase	Detailed information about why the error occurred, depending on the error type. This field can never be empty.

W3C EXTENDED LOG FILE FORMAT

Field	Appears As	Description	Default Y/N
Date	date	The date on which the activity occurred.	Y
Time	time	The time, in coordinated universal time (UTC), at which the activity occurred.	Y
Client IP Address	c-ip	The IP address of the client that made the request.	Y
User Name	cs-username	The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.	Y
Service Name and Instance Number	s-sitename	The Internet service name and instance number that was running on the client.	N
Server Name	s-computername	The name of the server on which the log file entry was generated.	N
Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.	Y
Server Port	s-port	The server port number that is configured for the service.	Y
Method	cs-method	The requested action, for example, a GET method.	Y
URI Stem	cs-uri-stem	The target of the action, e.g. default.htm	Y
URI Query	cs-uri-query	The query the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.	Y
HTTP Status	sc-status	The HTTP status code.	Y
Win32 Status	sc-win32-status	The Windows status code.	N
Bytes Sent	sc-bytes	The number of bytes that the server sent.	N
Bytes Received	cs-bytes	The number of bytes that the server received.	N
Time Taken	time-taken	The length of time that the action took, in milliseconds.	N
Protocol Version	cs-version	The protocol version — HTTP or FTP —that the client used.	N
Host	cs-host	The host header name, if any.	N
User Agent	cs(User-Agent)	The browser type that the client used.	Y