NAME

CURLOPT_SSL_CIPHER_LIST − specify ciphers to use for TLS

SYNOPSIS

#include <curl/curl.h>

CURLcode curl_easy_setopt(CURL *handle, CURLOPT_SSL_CIPHER_LIST, char *list);

DESCRIPTION

Pass a char *, pointing to a zero terminated string holding the list of ciphers to use for the SSL connection. The list must be syntactically correct, it consists of one or more cipher strings separated by colons. Commas or spaces are also acceptable separators but colons are normally used, !, - and + can be used as operators.

For OpenSSL and GnuTLS valid examples of cipher lists include 'RC4-SHA', ´SHA1+DES´, 'TLSv1' and 'DEFAULT'. The default list is normally set when you compile OpenSSL.

You'll find more details about cipher lists on this URL:

https://www.openssl.org/docs/apps/ciphers.html

For NSS, valid examples of cipher lists include 'rsa_rc4_128_md5', ´rsa_aes_128_sha´, etc. With NSS you don't add/remove ciphers. If one uses this option then all known ciphers are disabled and only those passed in are enabled.

You'll find more details about the NSS cipher lists on this URL:

http://git.fedorahosted.org/cgit/mod_nss.git/plain/docs/mod_nss.html#Directives

DEFAULT

NULL, use internal default

PROTOCOLS

All TLS based protocols: HTTPS, FTPS, IMAPS, POP3S, SMTPS etc.

EXAMPLE

TODO

AVAILABILITY

If built TLS enabled.

RETURN VALUE

Returns CURLE_OK if TLS is supported, CURLE_UNKNOWN_OPTION if not, or CURLE_OUT_OF_MEMORY if there was insufficient heap space.

SEE ALSO

CURLOPT_SSLVERSION(3), **CURLOPT_USE_SSL**(3),