

**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](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),