

**NAME**

CURLOPT\_SSL\_VERIFYSTATUS – verify the certificate's status

**SYNOPSIS**

```
#include <curl/curl.h>
```

```
CURLcode curl_easy_setopt(CURL *handle, CURLOPT_SSL_VERIFYSTATUS, long verify);
```

**DESCRIPTION**

Pass a long as parameter set to 1 to enable or 0 to disable.

This option determines whether libcurl verifies the status of the server cert using the "Certificate Status Request" TLS extension (aka. OCSP stapling).

Note that if this option is enabled but the server does not support the TLS extension, the verification will fail.

**DEFAULT**

0

**PROTOCOLS**

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

**EXAMPLE**

TODO

**AVAILABILITY**

Added in 7.41.0. This option is currently only supported by the OpenSSL, GnuTLS and NSS TLS backends.

**RETURN VALUE**

Returns CURLE\_OK if OCSP stapling is supported by the SSL backend, otherwise returns CURLE\_NOT\_BUILT\_IN.

**SEE ALSO**

CURLOPT\_SSL\_VERIFYHOST(3), CURLOPT\_SSL\_VERIFYPEER(3), CURLOPT\_CAINFO(3),