NAME

CURLOPT_SSL_VERIFYPEER − verify the peer's SSL certificate

SYNOPSIS

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

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

DESCRIPTION

Pass a long as parameter to enable or disable.

This option determines whether curl verifies the authenticity of the peer's certificate. A value of 1 means curl verifies; 0 (zero) means it does not.

When negotiating a TLS or SSL connection, the server sends a certificate indicating its identity. curl verifies whether the certificate is authentic, i.e. that you can trust that the server is who the certificate says it is. This trust is based on a chain of digital signatures, rooted in certification authority (CA) certificates you supply. curl uses a default bundle of CA certificates (the path for that is determined at build time) and you can specify alternate certificates with the *CURLOPT_CAINFO(3)* option or the *CURLOPT_CAPATH(3)* option.

When *CURLOPT_SSL_VERIFYPEER(3)* is enabled, and the verification fails to prove that the certificate is signed by a CA, the connection fails.

When this option is disabled (set to zero), the CA certificates are not loaded and the peer certificate verification is skipped.

Authenticating the certificate is not enough to be sure about the server. You typically also want to ensure that the server is the server you mean to be talking to. Use *CURLOPT_SSL_VERIFYHOST(3)* for that. The check that the host name in the certificate is valid for the hostname you are connecting to is done independently of the *CURLOPT_SSL_VERIFYPEER(3)* option.

WARNING: disabling verification of the certificate allows bad guys to man−in−the−middle the communication without you knowing it. Disabling verification makes the communication insecure. Having encryption on a transfer is not enough as you cannot be sure that you are communicating with the correct end−point.

When libcurl uses secure protocols it trusts responses and allows for example HSTS and Alt−Svc information to be stored and used subsequently. Disabling certificate verification can make libcurl trust and use such information from malicious servers.

DEFAULT

1 − enabled

PROTOCOLS

This functionality affects all TLS based protocols: HTTPS, FTPS, IMAPS, POP3S, SMTPS etc.

All TLS backends support this option.

EXAMPLE

```
int main(void)
{
  CURL *curl = curl_easy_init();
  if(curl) {
    CURLcode result;
    curl_easy_setopt(curl, CURLOPT_URL, "https://example.com");
```

```
    /* Set the default value: strict certificate check please */
    curl_easy_setopt(curl, CURLOPT_SSL_VERIFYPEER, 1L);

    result = curl_easy_perform(curl);
    curl_easy_cleanup(curl);
  }
}
```

AVAILABILITY

Added in curl 7.4.2

RETURN VALUE

curl_easy_setopt(3) returns a CURLcode indicating success or error.

CURLE_OK (0) means everything was OK, non−zero means an error occurred, see *libcurl−errors(3)*.

SEE ALSO

CURLINFO_CAINFO(3), **CURLINFO_CAPATH**(3), **CURLOPT_CAINFO**(3), **CURLOPT_PROXY_SSL_VERIFYHOST**(3), **CURLOPT_PROXY_SSL_VERIFYPEER**(3), **CURLOPT_SSL_VERIFYHOST**(3)