

**NAME**

CURLOPT\_CAINFO – path to Certificate Authority (CA) bundle

**SYNOPSIS**

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

```
CURLcode curl_easy_setopt(CURL *handle, CURLOPT_CAINFO, char *path);
```

**DESCRIPTION**

Pass a char \* to a zero terminated string naming a file holding one or more certificates to verify the peer with.

If *CURLOPT\_SSL\_VERIFYPEER(3)* is zero and you avoid verifying the server's certificate, *CURLOPT\_CAINFO(3)* need not even indicate an accessible file.

This option is by default set to the system path where libcurl's cacert bundle is assumed to be stored, as established at build time.

If curl is built against the NSS SSL library, the NSS PEM PKCS#11 module (libnsspem.so) needs to be available for this option to work properly.

(iOS and macOS only) If curl is built against Secure Transport, then this option is supported for backward compatibility with other SSL engines, but it should not be set. If the option is not set, then curl will use the certificates in the system and user Keychain to verify the peer, which is the preferred method of verifying the peer's certificate chain.

**DEFAULT**

Built-in system specific

**PROTOCOLS**

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

**EXAMPLE**

TODO

**AVAILABILITY**

For SSL engines that don't support certificate files the CURLOPT\_CAINFO option is ignored. Refer to <https://curl.haxx.se/docs/ssl-compared.html>

**RETURN VALUE**

Returns CURLE\_OK if the option is supported, CURLE\_UNKNOWN\_OPTION if not, or CURLE\_OUT\_OF\_MEMORY if there was insufficient heap space.

**SEE ALSO**

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