

NAME

SSL_CTX_set_client_CA_list, SSL_set_client_CA_list, SSL_CTX_add_client_CA, SSL_add_client_CA - set list of CAs sent to the client when requesting a client certificate

SYNOPSIS

```
#include <openssl/ssl.h>
```

```
void SSL_CTX_set_client_CA_list(SSL_CTX *ctx, STACK_OF(X509_NAME) *list);
void SSL_set_client_CA_list(SSL *s, STACK_OF(X509_NAME) *list);
int SSL_CTX_add_client_CA(SSL_CTX *ctx, X509 *cacert);
int SSL_add_client_CA(SSL *ssl, X509 *cacert);
```

DESCRIPTION

SSL_CTX_set_client_CA_list() sets the **list** of CAs sent to the client when requesting a client certificate for **ctx**.

SSL_set_client_CA_list() sets the **list** of CAs sent to the client when requesting a client certificate for the chosen **ssl**, overriding the setting valid for **ssl**'s SSL_CTX object.

SSL_CTX_add_client_CA() adds the CA name extracted from **cacert** to the list of CAs sent to the client when requesting a client certificate for **ctx**.

SSL_add_client_CA() adds the CA name extracted from **cacert** to the list of CAs sent to the client when requesting a client certificate for the chosen **ssl**, overriding the setting valid for **ssl**'s SSL_CTX object.

NOTES

When a TLS/SSL server requests a client certificate (see [SSL_CTX_set_verify\(3\)](#)), it sends a list of CAs, for which it will accept certificates, to the client.

This list must explicitly be set using *SSL_CTX_set_client_CA_list()* for **ctx** and *SSL_set_client_CA_list()* for the specific **ssl**. The list specified overrides the previous setting. The CAs listed do not become trusted (**list** only contains the names, not the complete certificates); use [SSL_CTX_load_verify_locations\(3\)](#) to additionally load them for verification.

If the list of acceptable CAs is compiled in a file, the [SSL_load_client_CA_file\(3\)](#) function can be used to help importing the necessary data.

SSL_CTX_add_client_CA() and *SSL_add_client_CA()* can be used to add additional items the list of client CAs. If no list was specified before using *SSL_CTX_set_client_CA_list()* or *SSL_set_client_CA_list()*, a new client CA list for **ctx** or **ssl** (as appropriate) is opened.

These functions are only useful for TLS/SSL servers.

RETURN VALUES

SSL_CTX_set_client_CA_list() and *SSL_set_client_CA_list()* do not return diagnostic information.

SSL_CTX_add_client_CA() and *SSL_add_client_CA()* have the following return values:

- 0 A failure while manipulating the STACK_OF(X509_NAME) object occurred or the X509_NAME could not be extracted from **cacert**. Check the error stack to find out the reason.
- 1 The operation succeeded.

EXAMPLES

Scan all certificates in **CAfile** and list them as acceptable CAs:

```
SSL_CTX_set_client_CA_list(ctx, SSL_load_client_CA_file(CAfile));
```

SEE ALSO

[ssl\(3\)](#), [SSL_get_client_CA_list\(3\)](#), [SSL_load_client_CA_file\(3\)](#), [SSL_CTX_load_verify_locations\(3\)](#)

COPYRIGHT

Copyright 2000-2016 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at

<<https://www.openssl.org/source/license.html>>.