

NAME

SSL_set_connect_state, SSL_set_accept_state - prepare SSL object to work in client or server mode

SYNOPSIS

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

void SSL_set_connect_state(SSL *ssl);

void SSL_set_accept_state(SSL *ssl);
```

DESCRIPTION

SSL_set_connect_state() sets **ssl** to work in client mode.

SSL_set_accept_state() sets **ssl** to work in server mode.

NOTES

When the SSL_CTX object was created with [SSL_CTX_new\(3\)](#), it was either assigned a dedicated client method, a dedicated server method, or a generic method, that can be used for both client and server connections. (The method might have been changed with [SSL_CTX_set_ssl_version\(3\)](#) or [SSL_set_ssl_method\(3\)](#).)

When beginning a new handshake, the SSL engine must know whether it must call the connect (client) or accept (server) routines. Even though it may be clear from the method chosen, whether client or server mode was requested, the handshake routines must be explicitly set.

When using the [SSL_connect\(3\)](#) or [SSL_accept\(3\)](#) routines, the correct handshake routines are automatically set. When performing a transparent negotiation using [SSL_write\(3\)](#) or [SSL_read\(3\)](#), the handshake routines must be explicitly set in advance using either [SSL_set_connect_state\(\)](#) or [SSL_set_accept_state\(\)](#).

RETURN VALUES

SSL_set_connect_state() and *SSL_set_accept_state()* do not return diagnostic information.

SEE ALSO

[ssl\(3\)](#), [SSL_new\(3\)](#), [SSL_CTX_new\(3\)](#), [LSSL_connect\(3\)](#), [SSL_accept\(3\)](#), [SSL_write\(3\)](#), [SSL_read\(3\)](#), [SSL_do_handshake\(3\)](#), [SSL_CTX_set_ssl_version\(3\)](#)

COPYRIGHT

Copyright 2001-2016 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>.