



*Full credit is given to the above companies including the OS that this PDF file was generated!*

## ***Red Hat Enterprise Linux Release 9.2 Manual Pages on 'SSL\_set\_mode.3ossl' command***

***\$ man SSL\_set\_mode.3ossl***

SSL\_CTX\_SET\_MODE(3ossl)      OpenSSL      SSL\_CTX\_SET\_MODE(3ossl)

### NAME

SSL\_CTX\_set\_mode, SSL\_CTX\_clear\_mode, SSL\_set\_mode, SSL\_clear\_mode,  
SSL\_CTX\_get\_mode, SSL\_get\_mode - manipulate SSL engine mode

### SYNOPSIS

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

long SSL_CTX_set_mode(SSL_CTX *ctx, long mode);

long SSL_CTX_clear_mode(SSL_CTX *ctx, long mode);

long SSL_set_mode(SSL *ssl, long mode);

long SSL_clear_mode(SSL *ssl, long mode);

long SSL_CTX_get_mode(SSL_CTX *ctx);

long SSL_get_mode(SSL *ssl);
```

### DESCRIPTION

SSL\_CTX\_set\_mode() adds the mode set via bit-mask in mode to ctx.

Options already set before are not cleared. SSL\_CTX\_clear\_mode() removes the mode set via bit-mask in mode from ctx.

SSL\_set\_mode() adds the mode set via bit-mask in mode to ssl. Options already set before are not cleared. SSL\_clear\_mode() removes the mode set via bit-mask in mode from ssl.

SSL\_CTX\_get\_mode() returns the mode set for ctx.

SSL\_get\_mode() returns the mode set for ssl.

### NOTES

The following mode changes are available:

## SSL\_MODE\_ENABLE\_PARTIAL\_WRITE

Allow `SSL_write_ex(..., n, &r)` to return with  $0 < r < n$  (i.e. report success when just a single record has been written). This works in a similar way for `SSL_write()`. When not set (the default), `SSL_write_ex()` or `SSL_write()` will only report success once the complete chunk was written. Once `SSL_write_ex()` or `SSL_write()` returns successful,  $r$  bytes have been written and the next call to `SSL_write_ex()` or `SSL_write()` must only send the  $n-r$  bytes left, imitating the behaviour of `write()`.

## SSL\_MODE\_ACCEPT\_MOVING\_WRITE\_BUFFER

Make it possible to retry `SSL_write_ex()` or `SSL_write()` with changed buffer location (the buffer contents must stay the same). This is not the default to avoid the misconception that nonblocking `SSL_write()` behaves like nonblocking `write()`.

## SSL\_MODE\_AUTO\_RETRY

During normal operations, non-application data records might need to be sent or received that the application is not aware of. If a non-application data record was processed, `SSL_read_ex(3)` and `SSL_read(3)` can return with a failure and indicate the need to retry with `SSL_ERROR_WANT_READ`. If such a non-application data record was processed, the flag `SSL_MODE_AUTO_RETRY` causes it to try to process the next record instead of returning.

In a nonblocking environment applications must be prepared to handle incomplete read/write operations. Setting `SSL_MODE_AUTO_RETRY` for a nonblocking BIO will process non-application data records until either no more data is available or an application data record has been processed.

In a blocking environment, applications are not always prepared to deal with the functions returning intermediate reports such as retry requests, and setting the `SSL_MODE_AUTO_RETRY` flag will cause the functions to only return after successfully processing an application data record or a failure.

Turning off `SSL_MODE_AUTO_RETRY` can be useful with blocking BIOs in

case they are used in combination with something like `select()` or `poll()`. Otherwise the call to `SSL_read()` or `SSL_read_ex()` might hang when a non-application record was sent and no application data was sent.

#### SSL\_MODE\_RELEASE\_BUFFERS

When we no longer need a read buffer or a write buffer for a given SSL, then release the memory we were using to hold it. Using this flag can save around 34k per idle SSL connection. This flag has no effect on SSL v2 connections, or on DTLS connections.

#### SSL\_MODE\_SEND\_FALLBACK\_SCSV

Send `TLS_FALLBACK_SCSV` in the ClientHello. To be set only by applications that reconnect with a downgraded protocol version; see [draft-ietf-tls-downgrade-scsv-00](#) for details.

DO NOT ENABLE THIS if your application attempts a normal handshake.

Only use this in explicit fallback retries, following the guidance in [draft-ietf-tls-downgrade-scsv-00](#).

#### SSL\_MODE\_ASYNC

Enable asynchronous processing. TLS I/O operations may indicate a retry with `SSL_ERROR_WANT_ASYNC` with this mode set if an asynchronous capable engine is used to perform cryptographic operations. See `SSL_get_error(3)`.

#### SSL\_MODE\_DTLS\_SCTP\_LABEL\_LENGTH\_BUG

Older versions of OpenSSL had a bug in the computation of the label length used for computing the endpoint-pair shared secret. The bug was that the terminating zero was included in the length of the label. Setting this option enables this behaviour to allow interoperability with such broken implementations. Please note that setting this option breaks interoperability with correct implementations. This option only applies to DTLS over SCTP.

All modes are off by default except for `SSL_MODE_AUTO_RETRY` which is on by default since 1.1.1.

#### RETURN VALUES

`SSL_CTX_set_mode()` and `SSL_set_mode()` return the new mode bit-mask

after adding mode.

SSL\_CTX\_get\_mode() and SSL\_get\_mode() return the current bit-mask.

#### SEE ALSO

ssl(7), SSL\_read\_ex(3), SSL\_read(3), SSL\_write\_ex(3) or SSL\_write(3),

SSL\_get\_error(3)

#### HISTORY

SSL\_MODE\_ASYNC was added in OpenSSL 1.1.0.

#### COPYRIGHT

Copyright 2001-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (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>>.

3.0.7                    2023-07-13            SSL\_CTX\_SET\_MODE(3ossl)