

**NAME**

SSL\_set\_retry\_verify - indicate that certificate verification should be retried

**SYNOPSIS**

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

```
int SSL_set_retry_verify(SSL *ssl);
```

**DESCRIPTION**

**SSL\_set\_retry\_verify()** should be called from the certificate verification callback on a client when the application wants to indicate that the handshake should be suspended and the control should be returned to the application. **SSL\_want\_retry\_verify(3)** will return 1 as a consequence until the handshake is resumed again by the application, retrying the verification step.

Please refer to **SSL\_CTX\_set\_cert\_verify\_callback(3)** for further details.

**NOTES**

The effect of calling **SSL\_set\_retry\_verify()** outside of the certificate verification callback on the client side is undefined.

**RETURN VALUES**

**SSL\_set\_retry\_verify()** returns 1 on success, 0 otherwise.

**EXAMPLES**

The following code snippet shows how to obtain the **SSL** object associated with the **X509\_STORE\_CTX** to call the **SSL\_set\_retry\_verify()** function:

```
int idx = SSL_get_ex_data_X509_STORE_CTX_idx();
SSL *ssl;

/* this should not happen but check anyway */
if (idx < 0
    || (ssl = X509_STORE_CTX_get_ex_data(ctx, idx)) == NULL)
    return 0;

if (/* we need to retry verification callback */)
    return SSL_set_retry_verify(ssl);

/* do normal processing of the verification callback */
```

**SEE ALSO**

`ssl(7)`, `SSL_connect(3)`, `SSL_CTX_set_cert_verify_callback(3)`, `SSL_want_retry_verify(3)`

**HISTORY**

`SSL_set_retry_verify()` was added in OpenSSL 3.0.2 to replace backwards incompatible handling of a negative return value from the verification callback.

**COPYRIGHT**

Copyright 2022 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>.