



*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\_CTX\_set1\_cert\_store.3ossl' command**

**`$ man SSL_CTX_set1_cert_store.3ossl`**

`SSL_CTX_SET_CERT_STORE(3ossl) OpenSSL SSL_CTX_SET_CERT_STORE(3ossl)`

### NAME

`SSL_CTX_set_cert_store`, `SSL_CTX_set1_cert_store`, `SSL_CTX_get_cert_store`

- manipulate X509 certificate verification storage

### SYNOPSIS

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

```
void SSL_CTX_set_cert_store(SSL_CTX *ctx, X509_STORE *store);
```

```
void SSL_CTX_set1_cert_store(SSL_CTX *ctx, X509_STORE *store);
```

```
X509_STORE *SSL_CTX_get_cert_store(const SSL_CTX *ctx);
```

### DESCRIPTION

`SSL_CTX_set_cert_store()` sets/replaces the certificate verification storage of `ctx` to/with `store`. If another `X509_STORE` object is currently set in `ctx`, it will be `X509_STORE_free()`ed.

`SSL_CTX_set1_cert_store()` sets/replaces the certificate verification storage of `ctx` to/with `store`. The store's reference count is incremented. If another `X509_STORE` object is currently set in `ctx`, it will be `X509_STORE_free()`ed.

`SSL_CTX_get_cert_store()` returns a pointer to the current certificate verification storage.

### NOTES

In order to verify the certificates presented by the peer, trusted CA certificates must be accessed. These CA certificates are made available via lookup methods, handled inside the `X509_STORE`. From the `X509_STORE`

the X509\_STORE\_CTX used when verifying certificates is created. Typically the trusted certificate store is handled indirectly via using SSL\_CTX\_load\_verify\_locations(3). Using the SSL\_CTX\_set\_cert\_store() and SSL\_CTX\_get\_cert\_store() functions it is possible to manipulate the X509\_STORE object beyond the SSL\_CTX\_load\_verify\_locations(3) call. Currently no detailed documentation on how to use the X509\_STORE object is available. Not all members of the X509\_STORE are used when the verification takes place. So will e.g. the verify\_callback() be overridden with the verify\_callback() set via the SSL\_CTX\_set\_verify(3) family of functions. This document must therefore be updated when documentation about the X509\_STORE object and its handling becomes available.

SSL\_CTX\_set\_cert\_store() does not increment the store's reference count, so it should not be used to assign an X509\_STORE that is owned by another SSL\_CTX.

To share X509\_STOREs between two SSL\_CTXs, use SSL\_CTX\_get\_cert\_store() to get the X509\_STORE from the first SSL\_CTX, and then use SSL\_CTX\_set1\_cert\_store() to assign to the second SSL\_CTX and increment the reference count of the X509\_STORE.

## RESTRICTIONS

The X509\_STORE structure used by an SSL\_CTX is used for verifying peer certificates and building certificate chains, it is also shared by every child SSL structure. Applications wanting finer control can use functions such as SSL\_CTX\_set1\_verify\_cert\_store() instead.

## RETURN VALUES

SSL\_CTX\_set\_cert\_store() does not return diagnostic output.

SSL\_CTX\_set1\_cert\_store() does not return diagnostic output.

SSL\_CTX\_get\_cert\_store() returns the current setting.

## SEE ALSO

ssl(7), SSL\_CTX\_load\_verify\_locations(3), SSL\_CTX\_set\_verify(3)

## COPYRIGHT

Copyright 2001-2016 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\_CERT\_STORE(3ossl)