



*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\_set0\_chain\_cert\_store.3ossl' command**

***\$ man SSL\_CTX\_set0\_chain\_cert\_store.3ossl***

SSL\_CTX\_SET1\_VERIFY\_CERT\_STORE(3ossl)OpenSSL\_CTX\_SET1\_VERIFY\_CERT\_STORE(3ossl)

### NAME

SSL\_CTX\_set0\_verify\_cert\_store, SSL\_CTX\_set1\_verify\_cert\_store,  
SSL\_CTX\_set0\_chain\_cert\_store, SSL\_CTX\_set1\_chain\_cert\_store,  
SSL\_set0\_verify\_cert\_store, SSL\_set1\_verify\_cert\_store,  
SSL\_set0\_chain\_cert\_store, SSL\_set1\_chain\_cert\_store,  
SSL\_CTX\_get0\_verify\_cert\_store, SSL\_CTX\_get0\_chain\_cert\_store,  
SSL\_get0\_verify\_cert\_store, SSL\_get0\_chain\_cert\_store - set certificate  
verification or chain store

### SYNOPSIS

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

```
int SSL_CTX_set0_verify_cert_store(SSL_CTX *ctx, X509_STORE *st);  
int SSL_CTX_set1_verify_cert_store(SSL_CTX *ctx, X509_STORE *st);  
int SSL_CTX_set0_chain_cert_store(SSL_CTX *ctx, X509_STORE *st);  
int SSL_CTX_set1_chain_cert_store(SSL_CTX *ctx, X509_STORE *st);  
int SSL_CTX_get0_verify_cert_store(SSL_CTX *ctx, X509_STORE **st);  
int SSL_CTX_get0_chain_cert_store(SSL_CTX *ctx, X509_STORE **st);  
  
int SSL_set0_verify_cert_store(SSL *ctx, X509_STORE *st);  
int SSL_set1_verify_cert_store(SSL *ctx, X509_STORE *st);
```

```
int SSL_set0_chain_cert_store(SSL *ctx, X509_STORE *st);
int SSL_set1_chain_cert_store(SSL *ctx, X509_STORE *st);
int SSL_get0_verify_cert_store(SSL *ctx, X509_STORE **st);
int SSL_get0_chain_cert_store(SSL *ctx, X509_STORE **st);
```

## DESCRIPTION

SSL\_CTX\_set0\_verify\_cert\_store() and SSL\_CTX\_set1\_verify\_cert\_store()  
set the certificate store used for certificate verification to st.

SSL\_CTX\_set0\_chain\_cert\_store() and SSL\_CTX\_set1\_chain\_cert\_store() set  
the certificate store used for certificate chain building to st.

SSL\_set0\_verify\_cert\_store(), SSL\_set1\_verify\_cert\_store(),  
SSL\_set0\_chain\_cert\_store() and SSL\_set1\_chain\_cert\_store() are similar  
except they apply to SSL structure ssl.

SSL\_CTX\_get0\_verify\_chain\_store(), SSL\_get0\_verify\_chain\_store(),  
SSL\_CTX\_get0\_chain\_cert\_store() and SSL\_get0\_chain\_cert\_store()  
retrieve the objects previously set via the above calls. A pointer to  
the object (or NULL if no such object has been set) is written to \*st.

All these functions are implemented as macros. Those containing a 1  
increment the reference count of the supplied store so it must be freed  
at some point after the operation. Those containing a 0 do not  
increment reference counts and the supplied store MUST NOT be freed  
after the operation.

## NOTES

The stores pointers associated with an SSL\_CTX structure are copied to  
any SSL structures when SSL\_new() is called. As a result SSL structures  
will not be affected if the parent SSL\_CTX store pointer is set to a  
new value.

The verification store is used to verify the certificate chain sent by the peer: that is an SSL/TLS client will use the verification store to verify the server's certificate chain and a SSL/TLS server will use it to verify any client certificate chain.

The chain store is used to build the certificate chain. Details of the chain building and checking process are described in "Certification Path Building" in openssl-verification-options(1) and "Certification Path Validation" in openssl-verification-options(1).

If the mode `SSL_MODE_NO_AUTO_CHAIN` is set or a certificate chain is configured already (for example using the functions such as `SSL_CTX_add1_chain_cert(3)` or `SSL_CTX_add_extra_chain_cert(3)`) then automatic chain building is disabled.

If the mode `SSL_MODE_NO_AUTO_CHAIN` is set then automatic chain building is disabled.

If the chain or the verification store is not set then the store associated with the parent `SSL_CTX` is used instead to retain compatibility with previous versions of OpenSSL.

## RETURN VALUES

All these functions return 1 for success and 0 for failure.

## SEE ALSO

`ssl(7)`, `SSL_CTX_add_extra_chain_cert(3)` `SSL_CTX_set0_chain(3)`  
`SSL_CTX_set1_chain(3)` `SSL_CTX_add0_chain_cert(3)`  
`SSL_CTX_add1_chain_cert(3)` `SSL_set0_chain(3)` `SSL_set1_chain(3)`  
`SSL_add0_chain_cert(3)` `SSL_add1_chain_cert(3)`  
`SSL_CTX_build_cert_chain(3)` `SSL_build_cert_chain(3)`

## HISTORY

These functions were added in OpenSSL 1.0.2.

## COPYRIGHT

Copyright 2013-2022 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>.

3.0.7                    2023-07SSL\_CTX\_SET1\_VERIFY\_CERT\_STORE(3ossl)