



## ***Red Hat Enterprise Linux Release 9.2 Manual Pages on 'SHA384\_Final.3oss1' command***

***\$ man SHA384\_Final.3oss1***

SHA256\_INIT(3oss1)            OpenSSL            SHA256\_INIT(3oss1)

### **NAME**

SHA1, SHA1\_Init, SHA1\_Update, SHA1\_Final, SHA224, SHA224\_Init,  
SHA224\_Update, SHA224\_Final, SHA256, SHA256\_Init, SHA256\_Update,  
SHA256\_Final, SHA384, SHA384\_Init, SHA384\_Update, SHA384\_Final, SHA512,  
SHA512\_Init, SHA512\_Update, SHA512\_Final - Secure Hash Algorithm

### **SYNOPSIS**

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

```
unsigned char *SHA1(const unsigned char *data, size_t count, unsigned char *md_buf);  
unsigned char *SHA224(const unsigned char *data, size_t count, unsigned char *md_buf);  
unsigned char *SHA256(const unsigned char *data, size_t count, unsigned char *md_buf);  
unsigned char *SHA384(const unsigned char *data, size_t count, unsigned char *md_buf);  
unsigned char *SHA512(const unsigned char *data, size_t count, unsigned char *md_buf);
```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining OPENSSL\_API\_COMPAT with a suitable version value, see openssl\_user\_macros(7):

```
int SHA1_Init(SHA_CTX *c);  
int SHA1_Update(SHA_CTX *c, const void *data, size_t len);
```

```
int SHA1_Final(unsigned char *md, SHA_CTX *c);
```

```
int SHA224_Init(SHA256_CTX *c);
```

```
int SHA224_Update(SHA256_CTX *c, const void *data, size_t len);
```

```
int SHA224_Final(unsigned char *md, SHA256_CTX *c);
```

```
int SHA256_Init(SHA256_CTX *c);
```

```
int SHA256_Update(SHA256_CTX *c, const void *data, size_t len);
```

```
int SHA256_Final(unsigned char *md, SHA256_CTX *c);
```

```
int SHA384_Init(SHA512_CTX *c);
```

```
int SHA384_Update(SHA512_CTX *c, const void *data, size_t len);
```

```
int SHA384_Final(unsigned char *md, SHA512_CTX *c);
```

```
int SHA512_Init(SHA512_CTX *c);
```

```
int SHA512_Update(SHA512_CTX *c, const void *data, size_t len);
```

```
int SHA512_Final(unsigned char *md, SHA512_CTX *c);
```

## DESCRIPTION

All of the functions described on this page except for SHA1(), SHA224(), SHA256(), SHA384() and SHA512() are deprecated. Applications should instead use EVP\_DigestInit\_ex(3), EVP\_DigestUpdate(3) and EVP\_DigestFinal\_ex(3), or the quick one-shot function EVP\_Q\_digest(3). SHA1(), SHA224(), SHA256(), SHA384(), and SHA512() can continue to be used. They can also be replaced by, e.g.,

```
(EVP_Q_digest(d, n, md, NULL, NULL, "SHA256", NULL) ? md : NULL)
```

SHA-1 (Secure Hash Algorithm) is a cryptographic hash function with a 160 bit output.

SHA1() computes the SHA-1 message digest of the n bytes at d and places it in md (which must have space for SHA\_DIGEST\_LENGTH == 20 bytes of

output). If md is NULL, the digest is placed in a static array. Note:  
setting md to NULL is not thread safe.

The following functions may be used if the message is not completely  
stored in memory:

SHA1\_Init() initializes a SHA\_CTX structure.

SHA1\_Update() can be called repeatedly with chunks of the message to be  
hashed (len bytes at data).

SHA1\_Final() places the message digest in md, which must have space for  
SHA\_DIGEST\_LENGTH == 20 bytes of output, and erases the SHA\_CTX.

The SHA224, SHA256, SHA384 and SHA512 families of functions operate in  
the same way as for the SHA1 functions. Note that SHA224 and SHA256 use  
a SHA256\_CTX object instead of SHA\_CTX. SHA384 and SHA512 use  
SHA512\_CTX. The buffer md must have space for the output from the SHA  
variant being used (defined by SHA224\_DIGEST\_LENGTH,  
SHA256\_DIGEST\_LENGTH, SHA384\_DIGEST\_LENGTH and SHA512\_DIGEST\_LENGTH).  
Also note that, as for the SHA1() function above, the SHA224(),  
SHA256(), SHA384() and SHA512() functions are not thread safe if md is  
NULL.

## RETURN VALUES

SHA1(), SHA224(), SHA256(), SHA384() and SHA512() return a pointer to  
the hash value.

SHA1\_Init(), SHA1\_Update() and SHA1\_Final() and equivalent SHA224,  
SHA256, SHA384 and SHA512 functions return 1 for success, 0 otherwise.

## CONFORMING TO

US Federal Information Processing Standard FIPS PUB 180-4 (Secure Hash

Standard), ANSI X9.30

## SEE ALSO

EVP\_Q\_digest(3), EVP\_DigestInit(3)

## HISTORY

All of these functions except SHA\*() were deprecated in OpenSSL 3.0.

## COPYRIGHT

Copyright 2000-2021 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            SHA256\_INIT(3ossl)