



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

### ***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_des\_ofb.3ossl'***

***\$ man EVP\_des\_ofb.3ossl***

EVP\_DES\_CBC(3ossl)            OpenSSL            EVP\_DES\_CBC(3ossl)

#### NAME

EVP\_des\_cbc, EVP\_des\_cfb, EVP\_des\_cfb1, EVP\_des\_cfb8, EVP\_des\_cfb64,  
EVP\_des\_ecb, EVP\_des\_ofb, EVP\_des\_edc, EVP\_des\_edc\_cbc,  
EVP\_des\_edc\_cfb, EVP\_des\_edc\_cfb64, EVP\_des\_edc\_ecb, EVP\_des\_edc\_ofb,  
EVP\_des\_edc3, EVP\_des\_edc3\_cbc, EVP\_des\_edc3\_cfb, EVP\_des\_edc3\_cfb1,  
EVP\_des\_edc3\_cfb8, EVP\_des\_edc3\_cfb64, EVP\_des\_edc3\_ecb,  
EVP\_des\_edc3\_ofb, EVP\_des\_edc3\_wrap - EVP DES cipher

#### SYNOPSIS

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

```
const EVP_CIPHER *EVP_ciphernam(void)
```

EVP\_ciphernam is used a placeholder for any of the described cipher functions, such as EVP\_des\_cbc.

## DESCRIPTION

The DES encryption algorithm for EVP.

`EVP_des_cbc()`, `EVP_des_ecb()`, `EVP_des_cfb()`, `EVP_des_cfb1()`,  
`EVP_des_cfb8()`, `EVP_des_cfb64()`, `EVP_des_ofb()`

DES in CBC, ECB, CFB with 64-bit shift, CFB with 1-bit shift, CFB with 8-bit shift and OFB modes.

None of these algorithms are provided by the OpenSSL default provider. To use them it is necessary to load either the OpenSSL legacy provider or another implementation.

`EVP_des_ede()`, `EVP_des_ede_cbc()`, `EVP_des_ede_cfb()`,  
`EVP_des_ede_cfb64()`, `EVP_des_ede_ecb()`, `EVP_des_ede_ofb()`

Two key triple DES in ECB, CBC, CFB with 64-bit shift and OFB modes.

`EVP_des_ede3()`, `EVP_des_ede3_cbc()`, `EVP_des_ede3_cfb()`,  
`EVP_des_ede3_cfb1()`, `EVP_des_ede3_cfb8()`, `EVP_des_ede3_cfb64()`,  
`EVP_des_ede3_ecb()`, `EVP_des_ede3_ofb()`

Three-key triple DES in ECB, CBC, CFB with 64-bit shift, CFB with 1-bit shift, CFB with 8-bit shift and OFB modes.

`EVP_des_ede3_wrap()`

Triple-DES key wrap according to RFC 3217 Section 3.

## RETURN VALUES

These functions return an `EVP_CIPHER` structure that contains the implementation of the symmetric cipher. See `EVP_CIPHER_meth_new(3)` for details of the `EVP_CIPHER` structure.

## SEE ALSO

`evp(7)`, `EVP_EncryptInit(3)`, `EVP_CIPHER_meth_new(3)`

## COPYRIGHT

Copyright 2017-2021 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                    EVP\_DES\_CBC(3ossl)