EFArmor Manual

EFArmor Standard Version 1.5.0

Table of contents

1. Introduction

EFArmor is one file encryption and decryption software. It uses standard cryptography algorithms and security protocol to encrypt files. Anyone cannot modify, read and use these encrypted files.

EFArmor uses RSA (default key size is 1024) by default to create security key. It is necessary to setup one **passphrase** to protect it. The security key is saved to your computer automatically. But we don't save the **passphrase** since security reason. So, you must remember and save it by yourself.

EFArmor's core uses the AES (Advanced Encryption Standard) and PGP like protocol to complete file encryption action.

Feature list of EFArmor version 1.5.0:

File explorer: There is one simple built-in file explorer helping to select files/folders.

Keyrings: It helps you to create key encrypting and decrypting files.

Encryption/Decryption panel: The central operation panel by which you encrypt and decrypt files.

Checking file integrity: Check the integrity of files from website/network and so on.

Supported operations system:

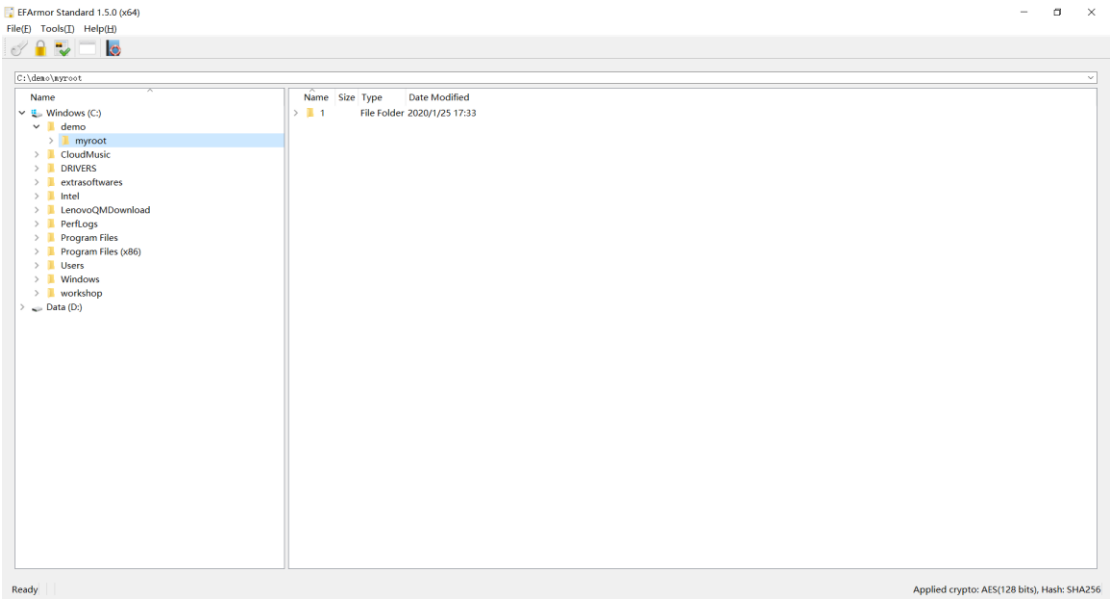
Windows platform: Windows Vista or above. The recommended one is Win10.

Mac: Support the latest macOS - macOS Catalina.

2. User guide

There are only 3 steps to use EFArmor.

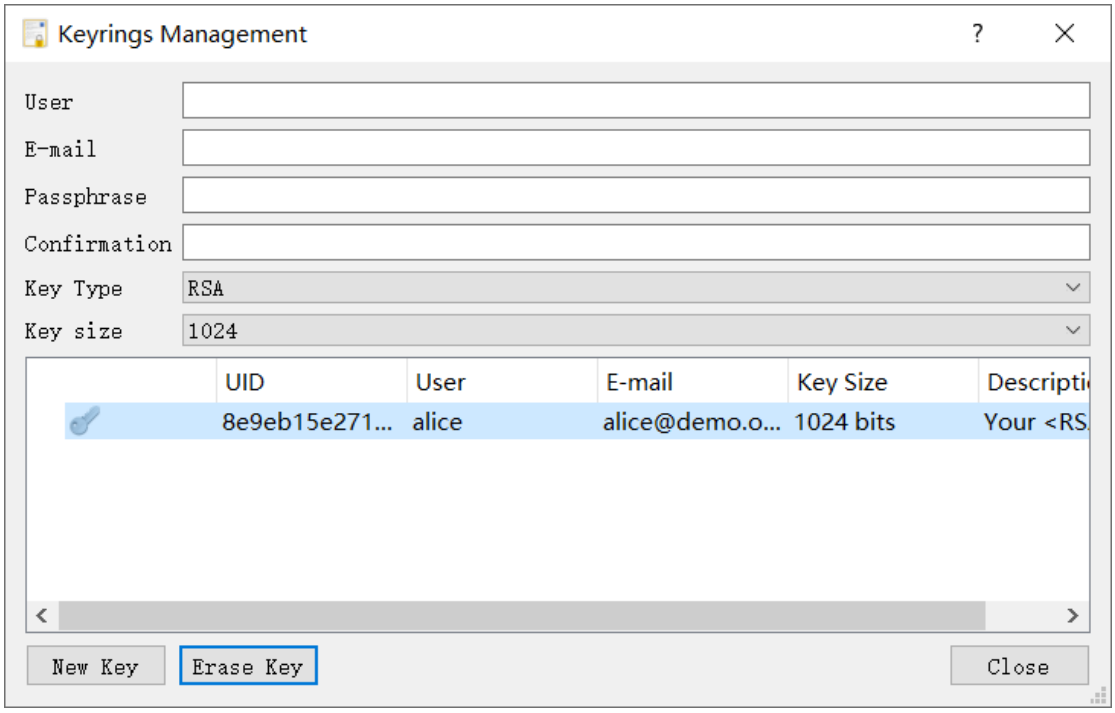
- ✓ Create one security key – Manage Security Keys.
- ✓ Import files to be encrypted/decrypted – Import files.
- ✓ Execute encryption/decryption – Encrypt/Decrypt files.



2.1 Manage Security keys

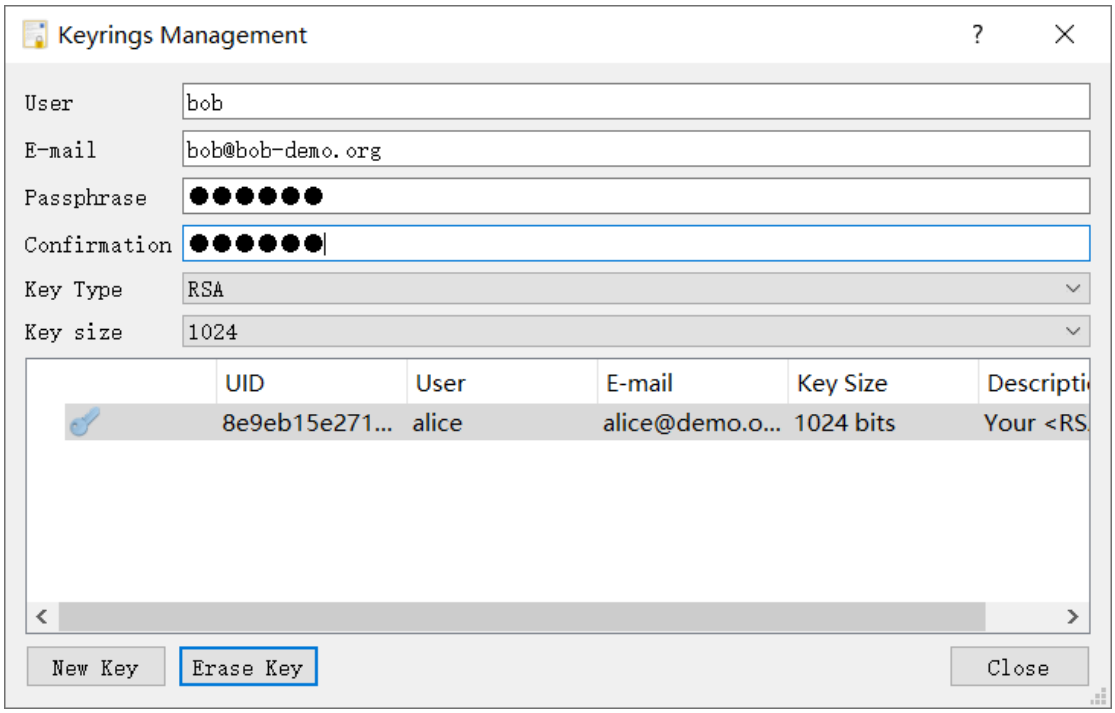
2.1.1 Create security key and setup master phrase to protect it.

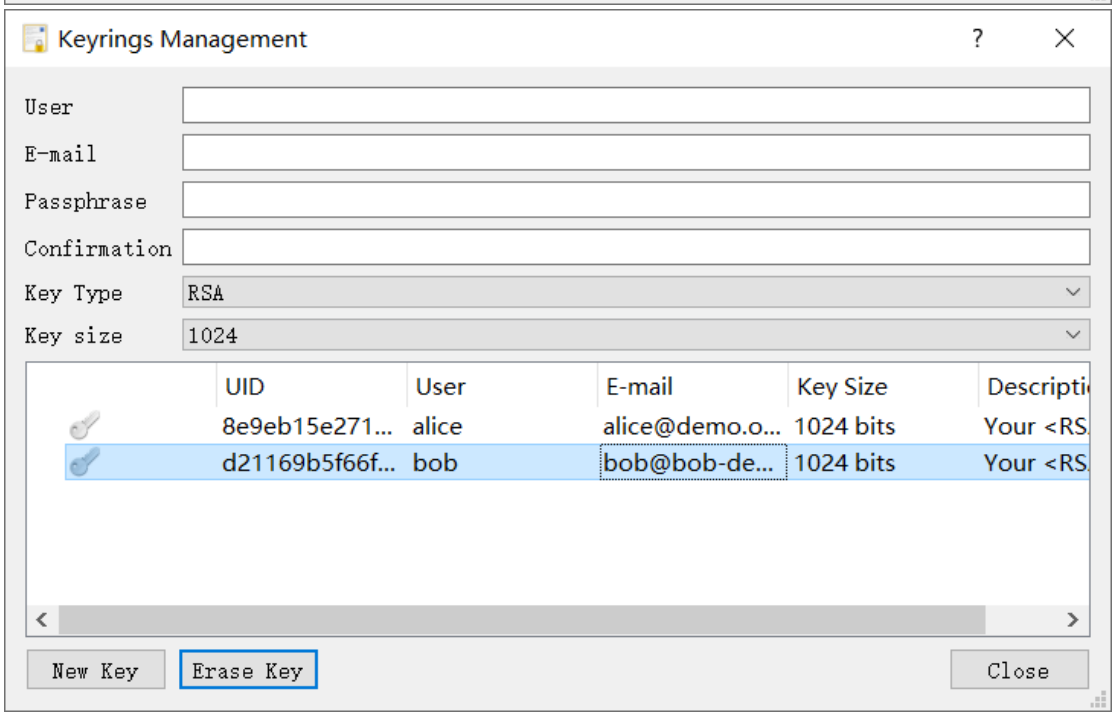
Open menu item: Tools->Keyrings



Please fill username, e-mail, passphrase, key type and key size in this dialog, then press the button named 'New Key' to create one new security key.

For example: Create one new key named 'bob'.





Note:

a) The 'passphrase' is the used to protect this security key.

b) **Please remember/save the 'passphrase' by yourself**. It is impossible to decrypt files which is protected with 'passphrase' if you forget it.

A. The EFArmor identify this security key by username and e-mail.

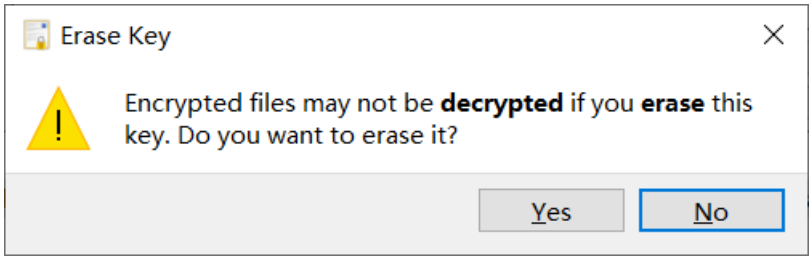
B. The 'UID' is generated through username and e-mail automatically. It is solely.

C. It is possible to create multi security keys. But their usernames and e-mails should be different.

2.1.2 Erase security key

You can select one security key in the Keyring Management dialog and press button ‘Erase Key’. A warning dialog is pop up and ask you to confirm the erasing action.

The selected security key is erased if you press ‘Yes’ button.



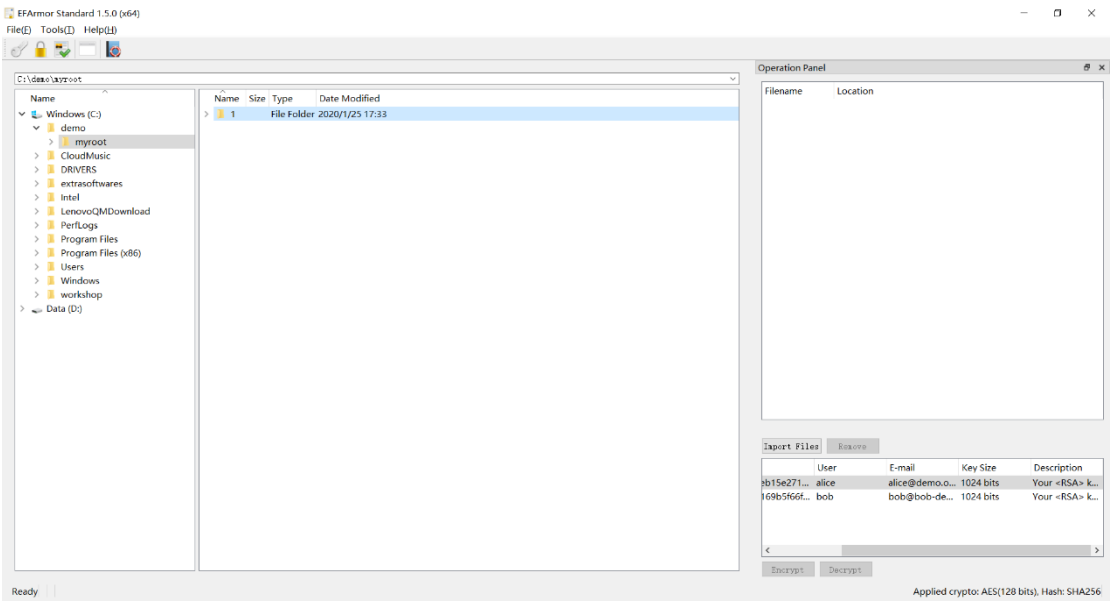
Note:

a) It is impossible to recovery the removed security key.

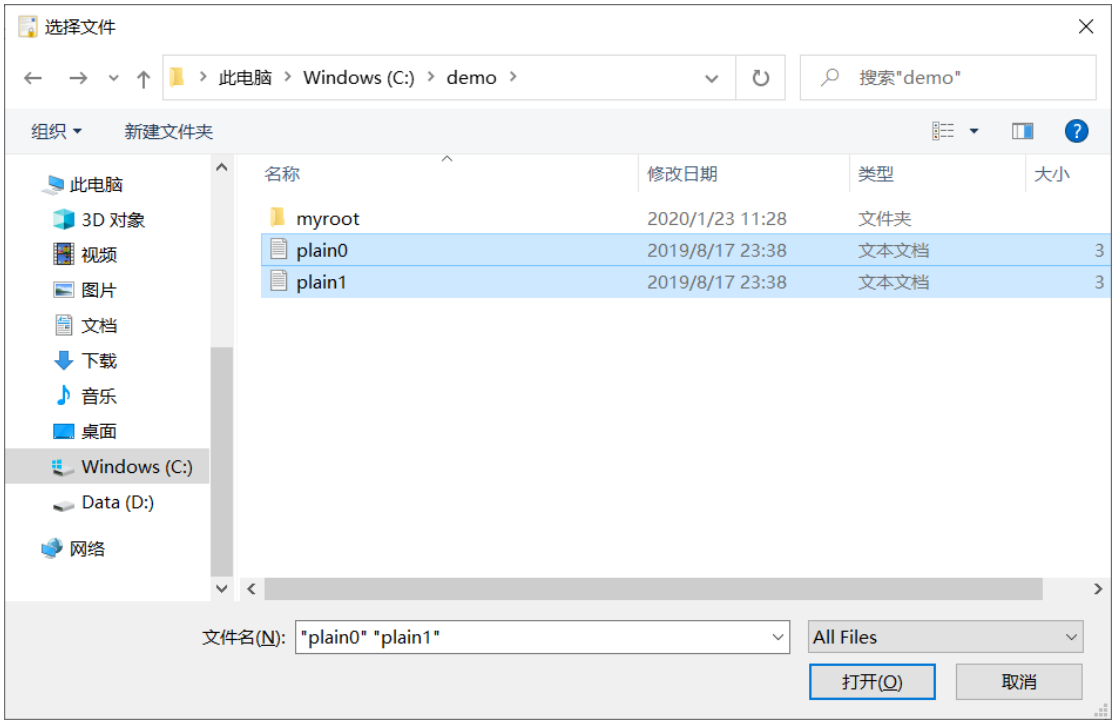
b) All files encrypted with the **security key** are not been decrypted if it is erased.

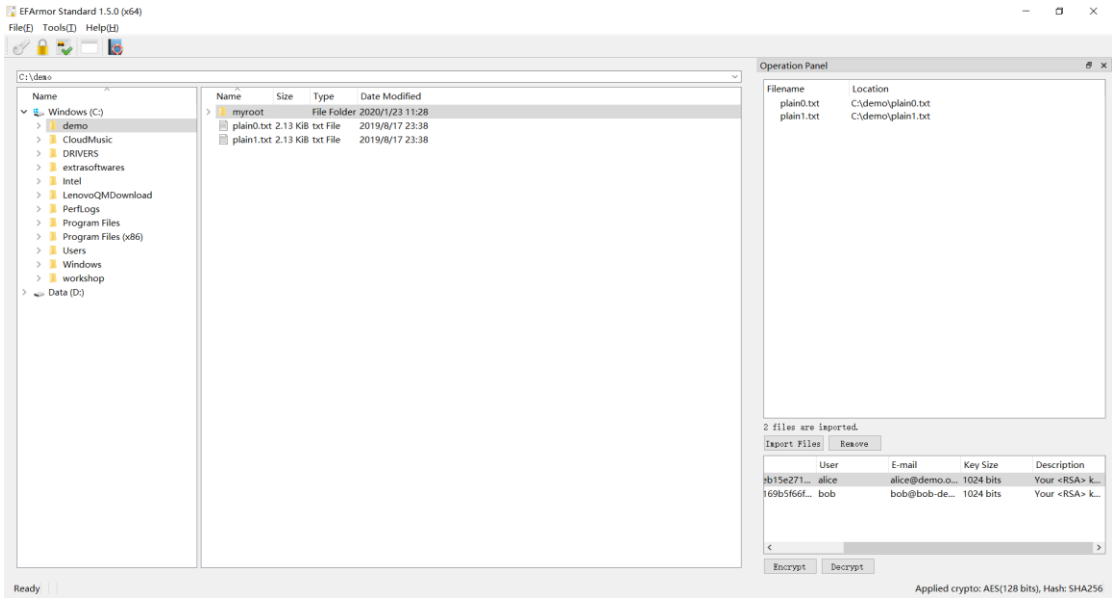
2.2 Import files

2.2.1 Open menu item -> Operation Panel

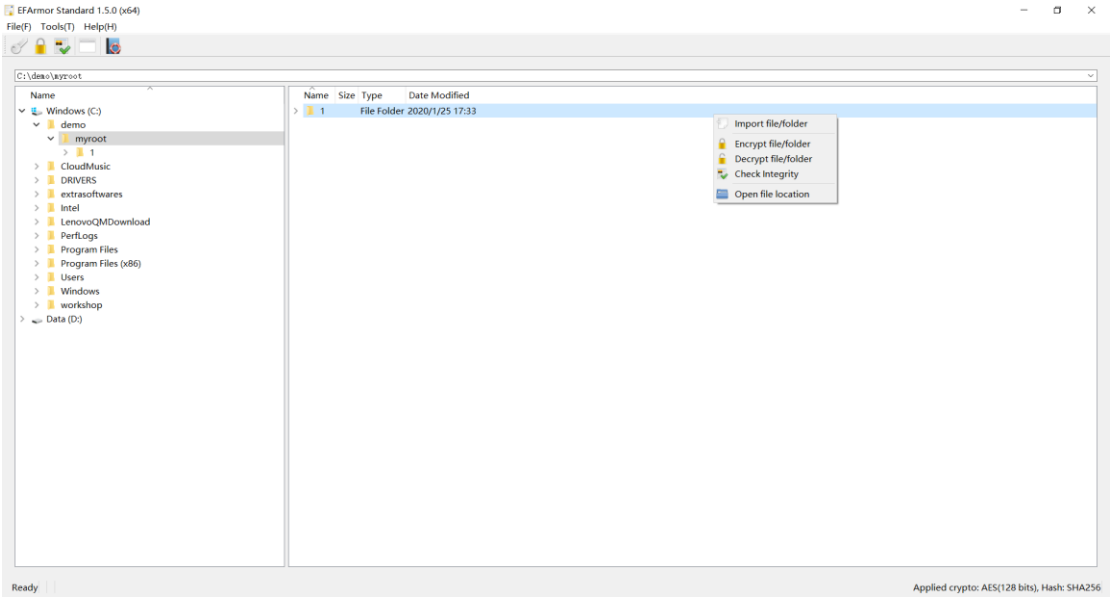


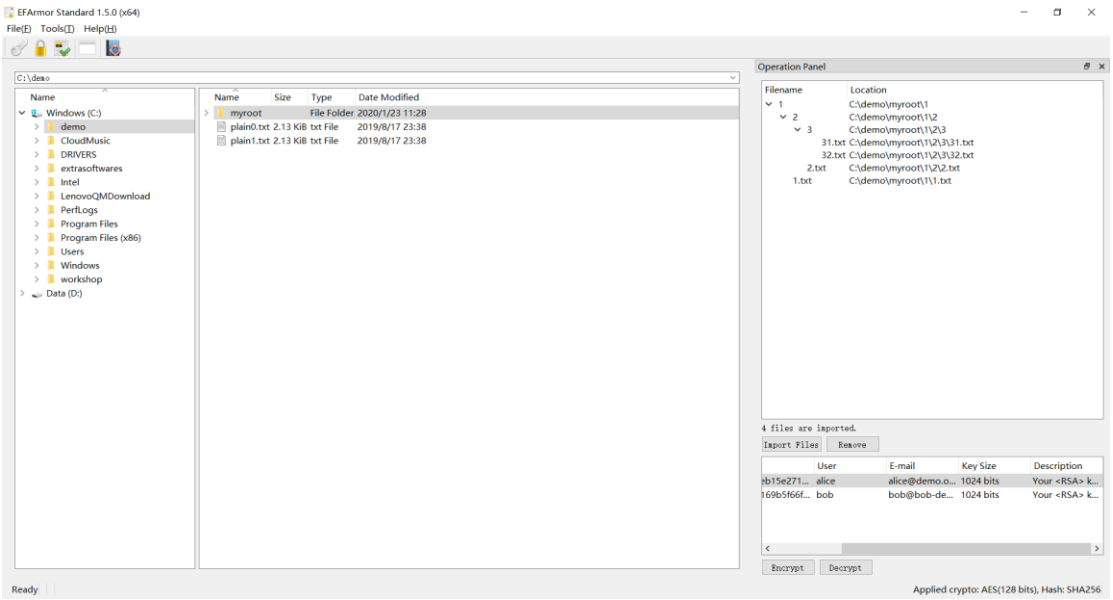
Press ‘Import Files’ to open files selection dialog to select files imported.





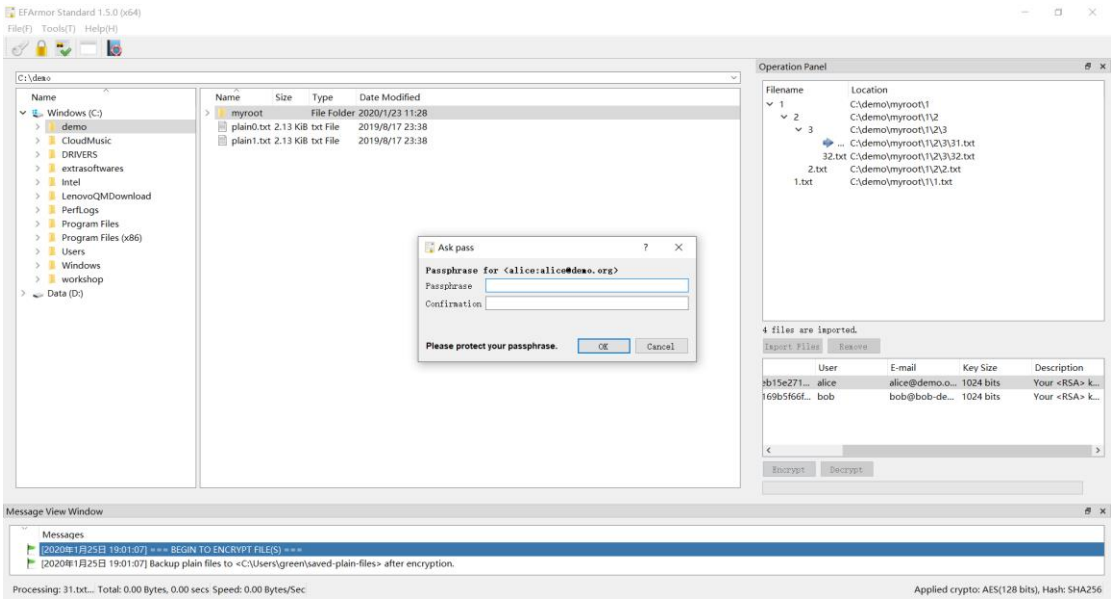
2.2.2 Click right mouse in file selection area to select “Import file/folder” menu item.



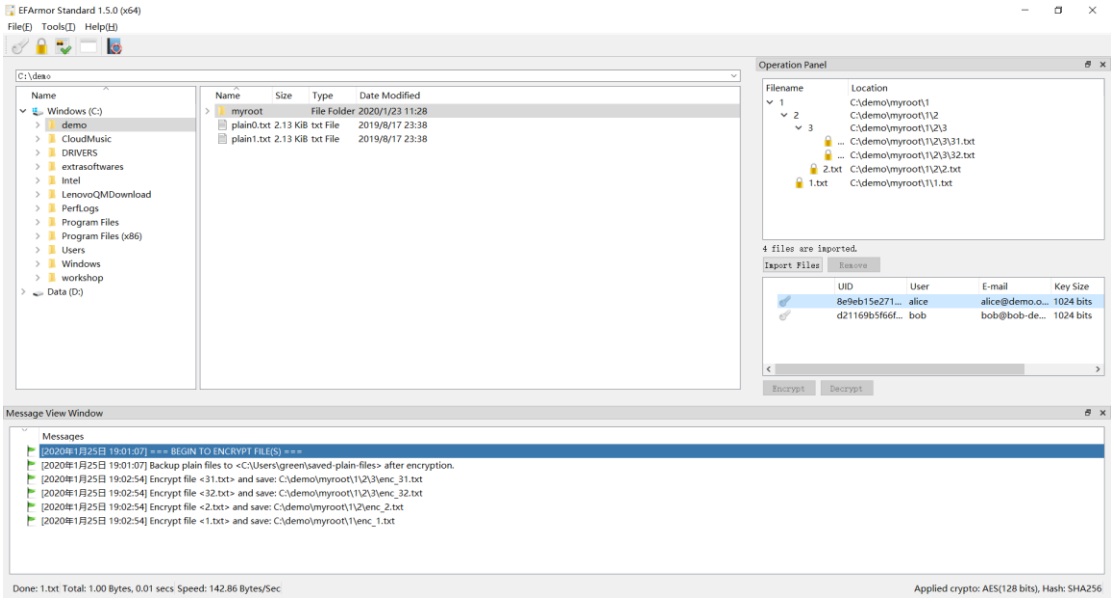


2.3 Encrypt and decrypt files

Press button named ‘Encrypt’ and ‘Decrypt’ to after importing files. EFArmor pops up one dialog and ask you to input proper ‘Passphrase’.



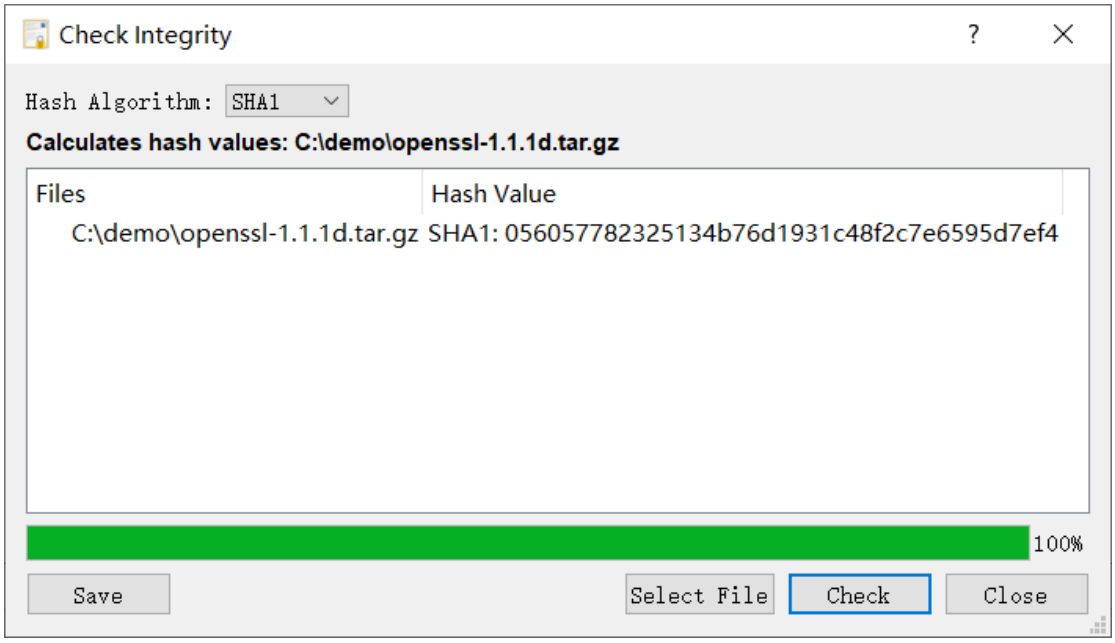
After encryption ends:



2.4 Check integrity of files

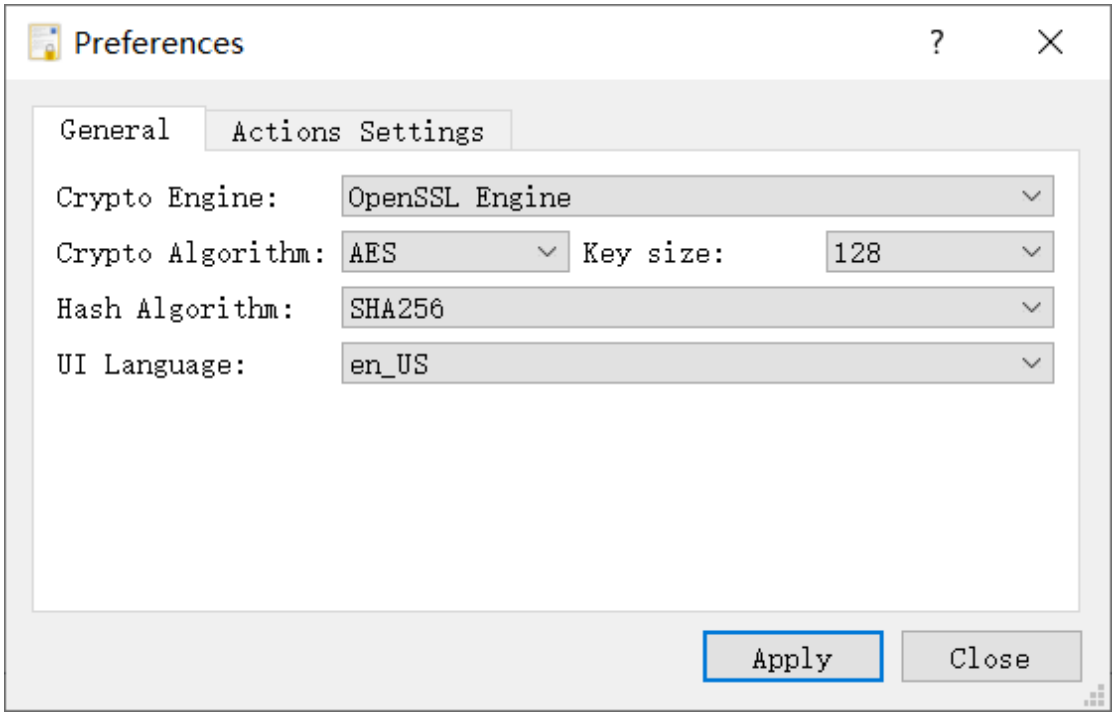
Open menu item: Tools -> Check Integrity

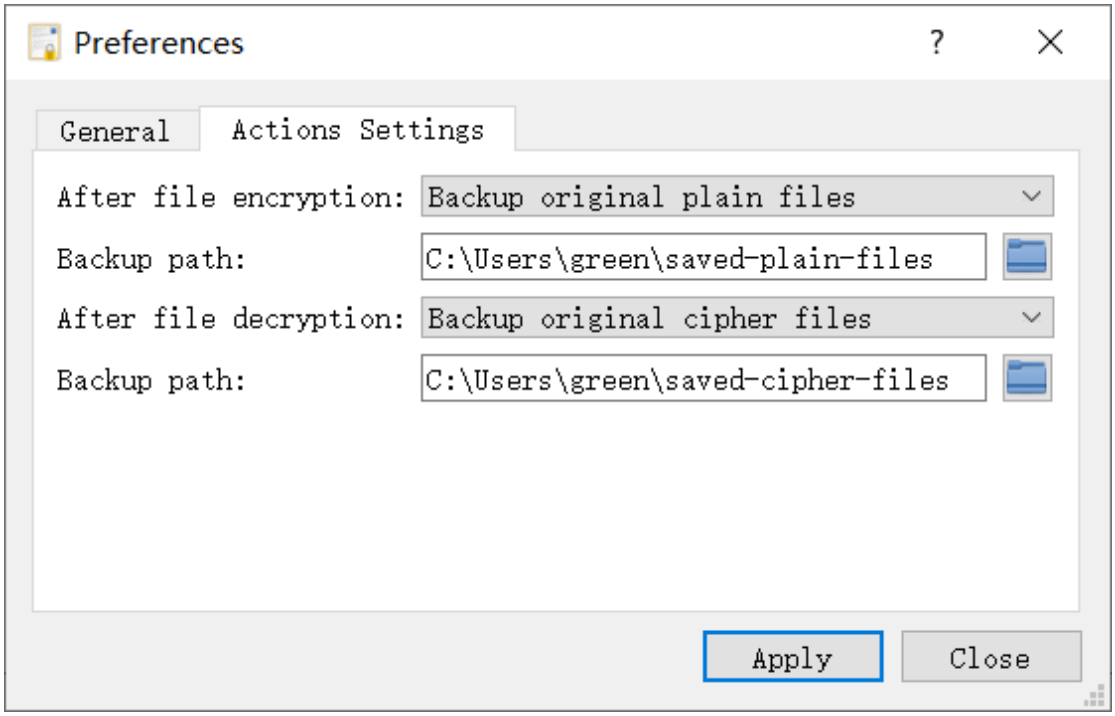
Select files and Press ‘Check’. You can view and save final results after checking ends.



2.5 Preference

Open it with main menu item: Tool -> Preferences





There are three types of settings can be adjusted:

A. Adjust cryptography parameters
   a) Cryptography algorithms and key size.
   b) Hash algorithms used in encryption action.

B. Operations after encryption.
   a) Keep original plain files unchanged
      All plain files are still on original folder after encryption ends.
   b) Backup original plain files
      EFArmor backups all original plain files to one folder after encryption ends.
   c) Only keep new created cipher files
      EFArmor removes all original plain files after encryption ends.

C. Operations after decryption
   a) Keep original cipher files unchanged
      All cipher files are still on original folder after decryption ends.
   b) Backup original cipher files.
      EFArmor backups all original cipher files to one folder after decryption ends.
   c) Only keep new created plain files
      EFArmor removes all original cipher files after decryption ends.

D. Languages of UI
   There are three types of languages supported now. They are:
   a) en_US: English language.
   b) zh_CN: Chinese simplified language.
   c) zh_TW: Chinese traditional language.
   It needs to restart EFArmor to let new language effect.

3. Introduction of cryptography library used in EFArmor

EFArmor version 1.5.0 uses OpenSSL as the crypto engine. So, EFArmor can run on both Windows and Mac platform.

Algorithms used in EFArmor v1.5.0

Algorithms name	Usage	Note
RSA	Used in security key	There are two types of key size: 1024 bits, 2048 bits. The default one is 1024 bits. Default key size is 1024 bits.
RC2	Used in data encryption and decryption.	Key size supported: 40/64/128 bits
RC4		Key size supported: 40/128 bits
AES		Key size supported: 128/192/256 bits.
DES		Key size supported: 56 bits.
DESX		Key size supported: 184 bits.
BLOWFISH		Key size supported: 128 bits.
CAST5		Key size supported: 128 bits.
IDEA		Key size supported: 128 bits.
3DES		Key size supported: 168 bits.
RNG	Random-number generator algorithm.	遵守的标准： FIPS 186-2, FIPS 140-2, NIST SP 800-90
MD2	MD2 hash algorithm.	Size: 128 bits.
MD4	MD4 hash algorithm	
MD5	MD5 hash algorithm	
SHA1	Secure Hash Algorithm	Size: 160 bits.
SHA2	Secure Hash Algorithm 2	Size: 256/384/512 bits

4. FAQ

1. Why do I fail to encrypt files stored in U disk?
   Please copy files to your computer's disk and try to encrypt them again.
2. Which OS does EFArmor support?
   EFArmor supports both Windows and Mac since version 1.5.0.
3. What's the roadmap of EFArmor project?
   Please visit our project website: https://github.com/EFArmorSupport/EFArmor

5. Acknowledge

EFArmor uses following third components:

A. The zlib library, version is 1.2.11
B. The Qt 5.13.0.
C. The oxygen-icons and KDE organization (https://kde.org).
D. OpenSSL 1.1.1d.

Please read files stored in the folder 3RDLicenses.