MKey User’ s Manual

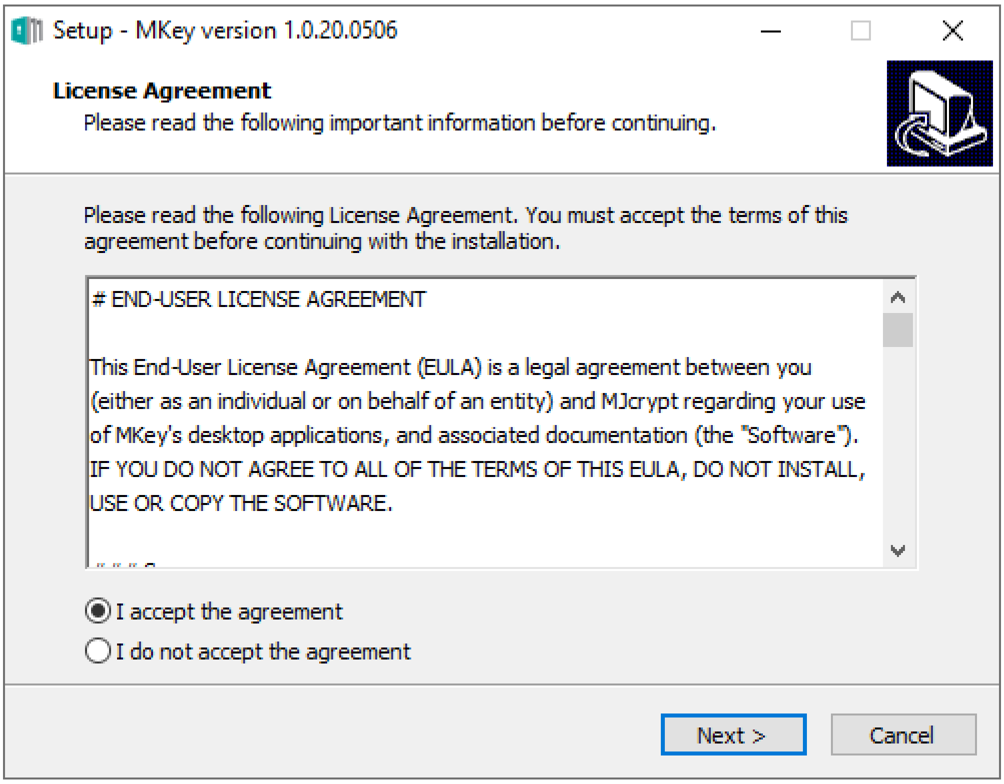
Ver 2.03

Directory

MKey Installation

The MKey application will be copied on the MKEY disk as a compressed file, such as 1.0.20.0506_MKeySetup.zip. You can also download the latest version of the application on the MJcrypt website, https://www.mjcrypt.com/tw/download. Directly double-click the application compressed file with the mouse to install the application. Some anti-virus software will block the executable file (.exe) or the Windows dynamic link file (.dll). Please allow execution, or temporarily stop the antivirus software during the installation process if there is anti-virus software block program in installation directory (usually "C: \ Program Files \ MKEY"), executable file (.exe) or Windows dynamic link file. Open the antivirus software after the installation is completed.

You must first accept the contents of the license agreement to continue the installation.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

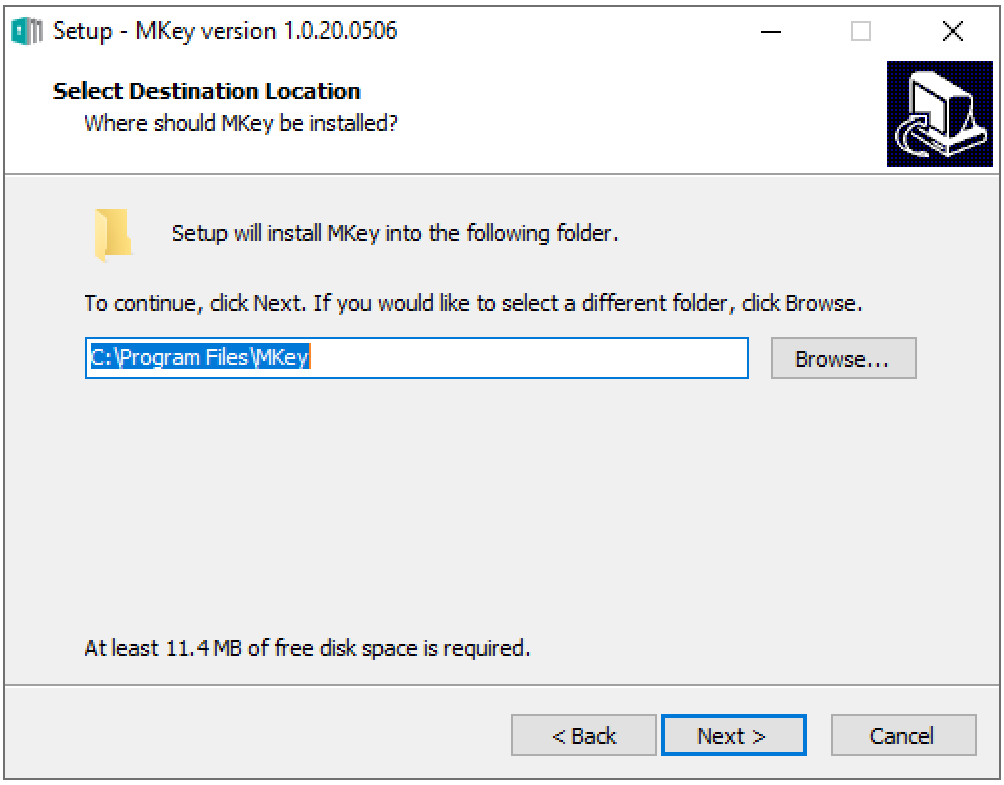
END-USER LICENSE AGREEMENT

This End-User License Agreement (EULA) is a legal agreement between you (either as an individual or on behalf of an entity) and MJcrypt regarding your use of MKey's desktop applications, and associated documentation (the "Software"). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS EULA, DO NOT INSTALL, USE OR COPY THE SOFTWARE.

● I accept the agreement

○ I do not accept the agreement

It is recommended to install the MKey program in the "C: \ Program Files \ MKey" directory to maintain the consistency of the windows execution program.



Setup - MKey version 1.0.20.0506

Select Destination Location

Where should MKey be installed?

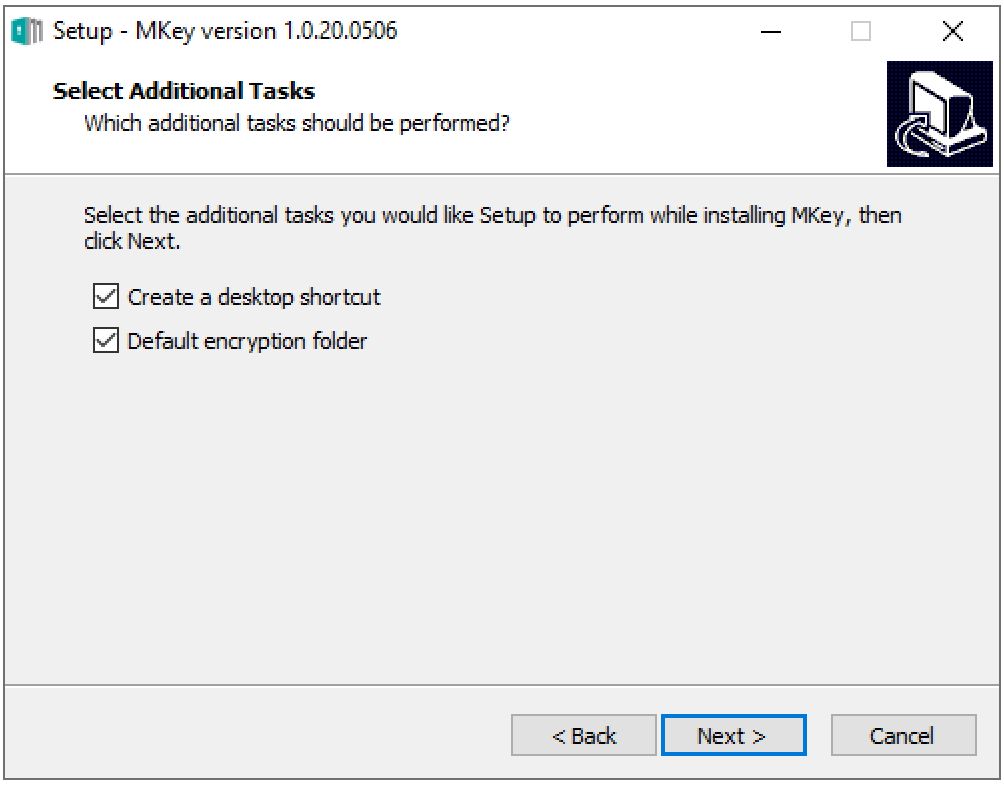
Setup will install MKey into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\MKey

At least 11.4 MB of free disk space is required.

To select “Create a desktop shortcut” will create an icon on the desktop for easy operation. To select “Default encryption folder” will be pre-built with an encrypted data folder corresponding to a plain text virtual disk in “C: \ Users \ user \ Documents \ MKey” during installation. It can be used directly after installation.



Setup - MKey version 1.0.20.0506

Select Additional Tasks

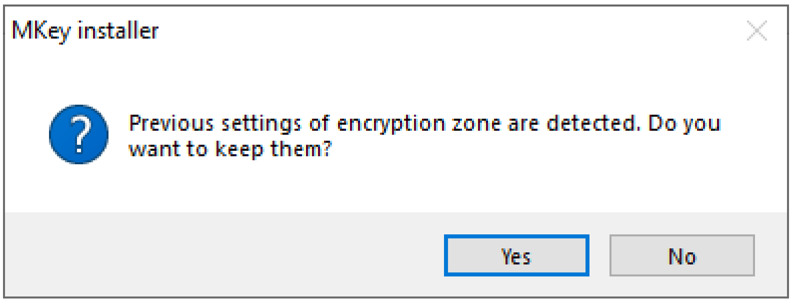
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing MKey, then click Next.

☑ Create a desktop shortcut

☑ Default encryption folder

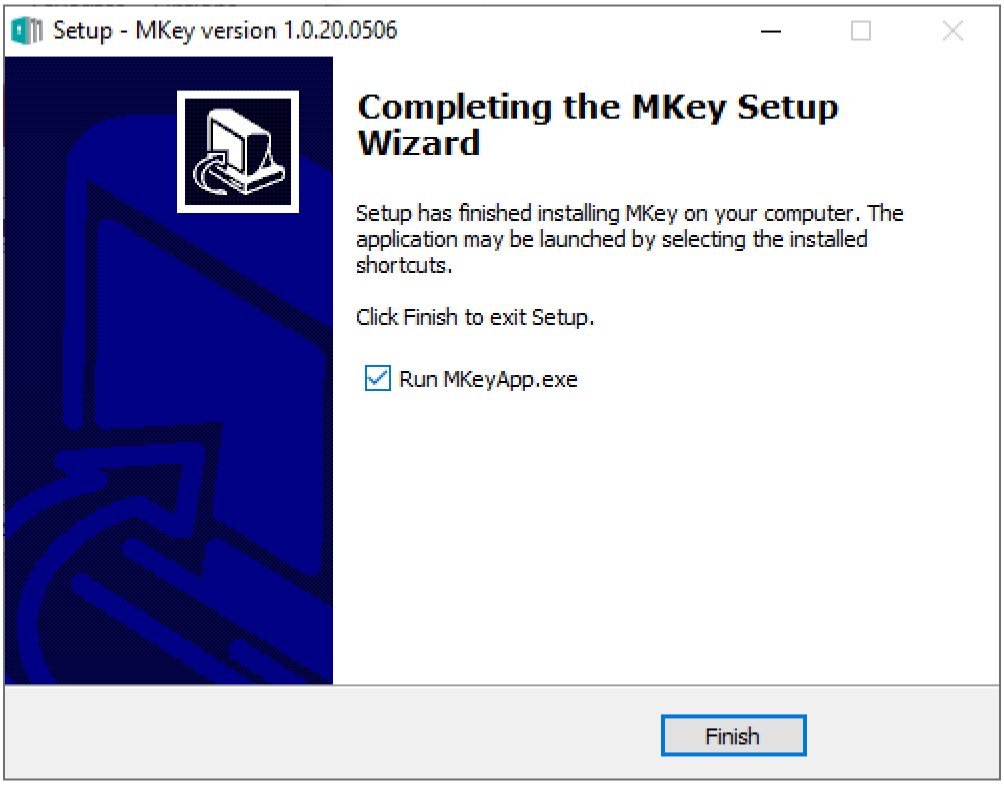
If you are not installing for the first time, choose keep the previous setting of encryption zone may reduce the trouble of re-setting.



MKey installer

Previous settings of encryption zone are detected. Do you want to keep them?

Press Finish to complete the installation.



Setup - MKey version 1.0.20.0506

Completing the MKey Setup Wizard

Setup has finished installing MKey on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

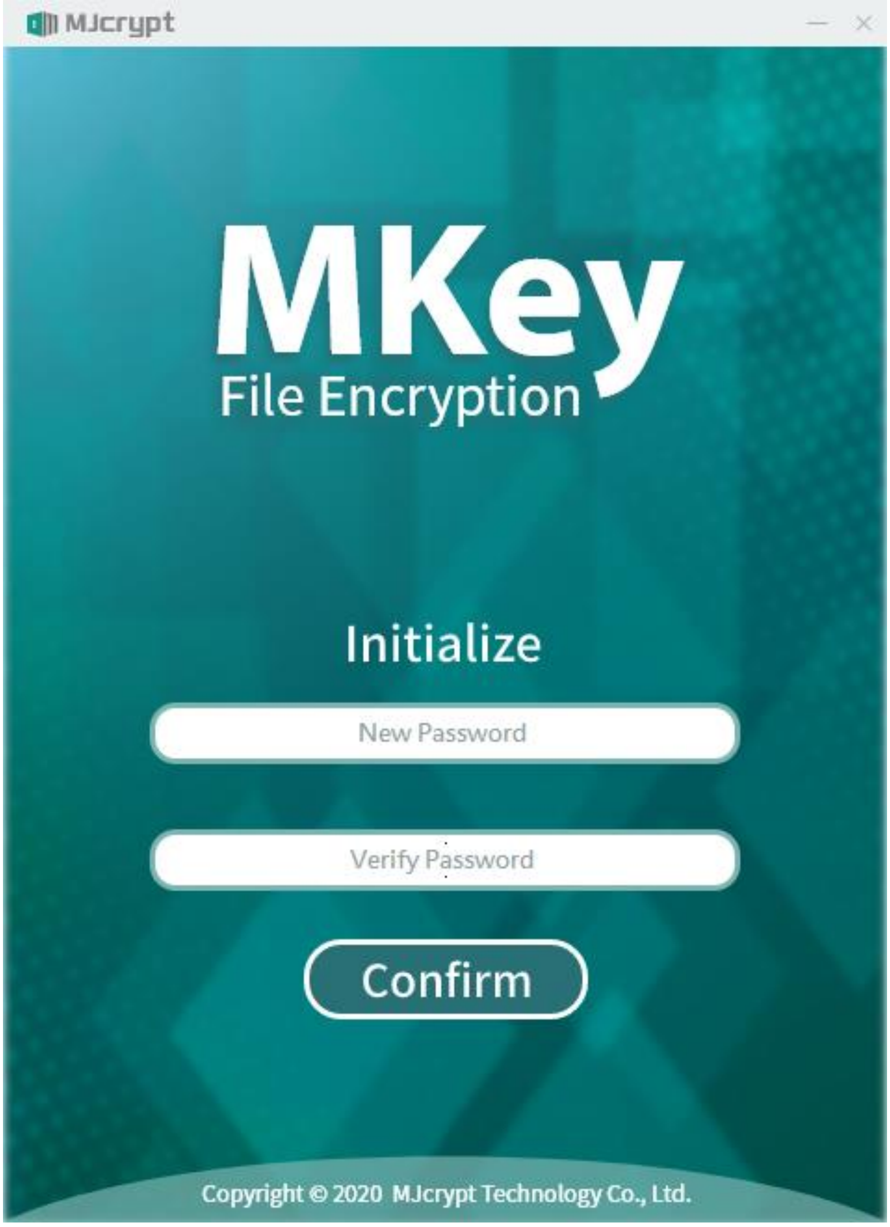
☑ Run MKeyApp.exe

MKey Setup

Initialize

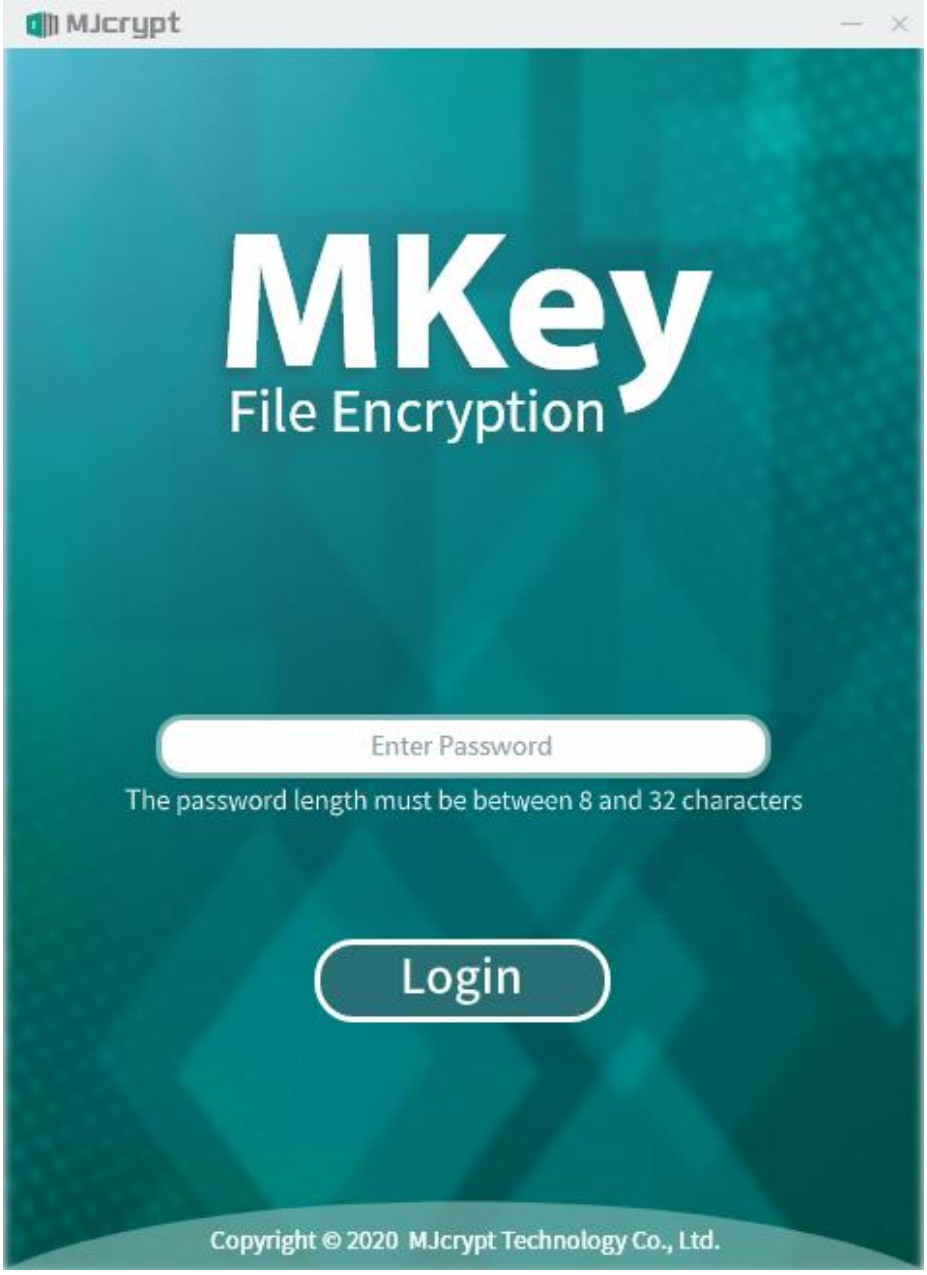
When MKey hardware is used for the first time, the user will be required to set a password to initialize MKey. This password is set by the user. The password must be the same in both fields before confirm. The password setting digits are 8 ~ 32 digits.

After MKey executes "Revert" in "Settings", MKEY will be regarded as the initialize state after being re-plugged and will be required to initialize the password.



Login Page

As long as the MKey application detects that the hardware is inserted into the USB port, it will automatically pop up the login page. As long as the user enters the correct password, he can enter the user's main screen area for all encryption and decryption function.


MJcrypt
MKey
File Encryption
Enter Password
The password length must be between 8 and 32 characters
Login
Copyright © 2020 MJcrypt Technology Co., Ltd.

Encryption Folder

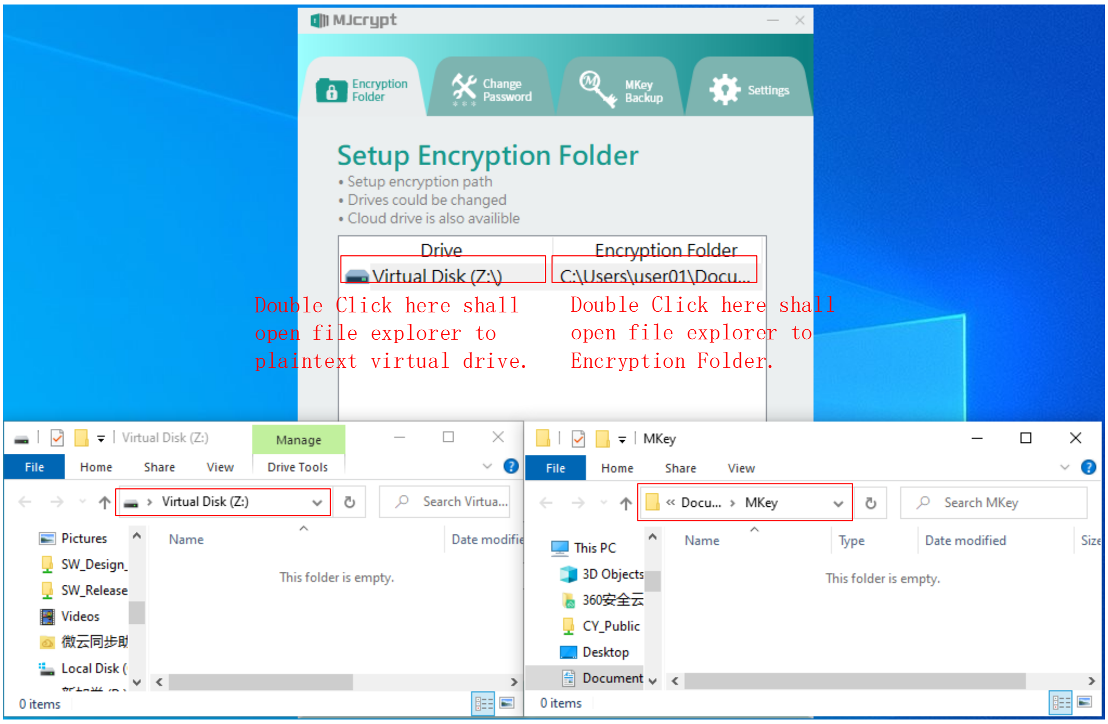
There are two ways to use encryption and decryption after correct login.

The first is the encryption and decryption method is the mapping method by the "Encryption Folder" to the virtual disk in the "Drive". User store plain text file in "Drive" may cause encrypted file is stores in "Encryption Folder" after the correct login. User can see the encrypted data in encryption folder and the plain text file in the virtual drive at the same time.

The second type is the right key encryption and decryption function. The data only exists in the form of encryption or decryption. For its setting and usage, please refer to "Settings".

The following setting is the first encryption / decryption setting method regarding the "Encryption Folder" to the virtual disk "Drive". If user select "Default encryption folder" during the installation process, a set of encryption settings will be preset after the installation is completed. User can use it directly after installation. Move the mouse to ” Drive” or the corresponding “Encryption Folder” position then double-click mouse to pop up the explorer window of the plain text or the encrypted folder. The plain text editing area only appears after inserting MKey and entering the correct password. If users want to copy or edit files, please edit in the virtual disk area in plain text. ***The encrypted data in the encryption folder is an ever-present area, but it exists in the form of AES256 encryption, and the user must not edit it arbitrarily, otherwise the data cannot be decoded.*** The encrypted files in encryption folder is generated according to the encoding of each MKey hardware. The AES encoding key is store in MKey hardware, so different MKey hardware can’t decrypt the encrypted data with each other.

The user can copy the files in encryption folder to other directories of but cannot edit them. The copied files can also be decrypted by using the same MKey after entering the correct password.



Setup Encryption Folder

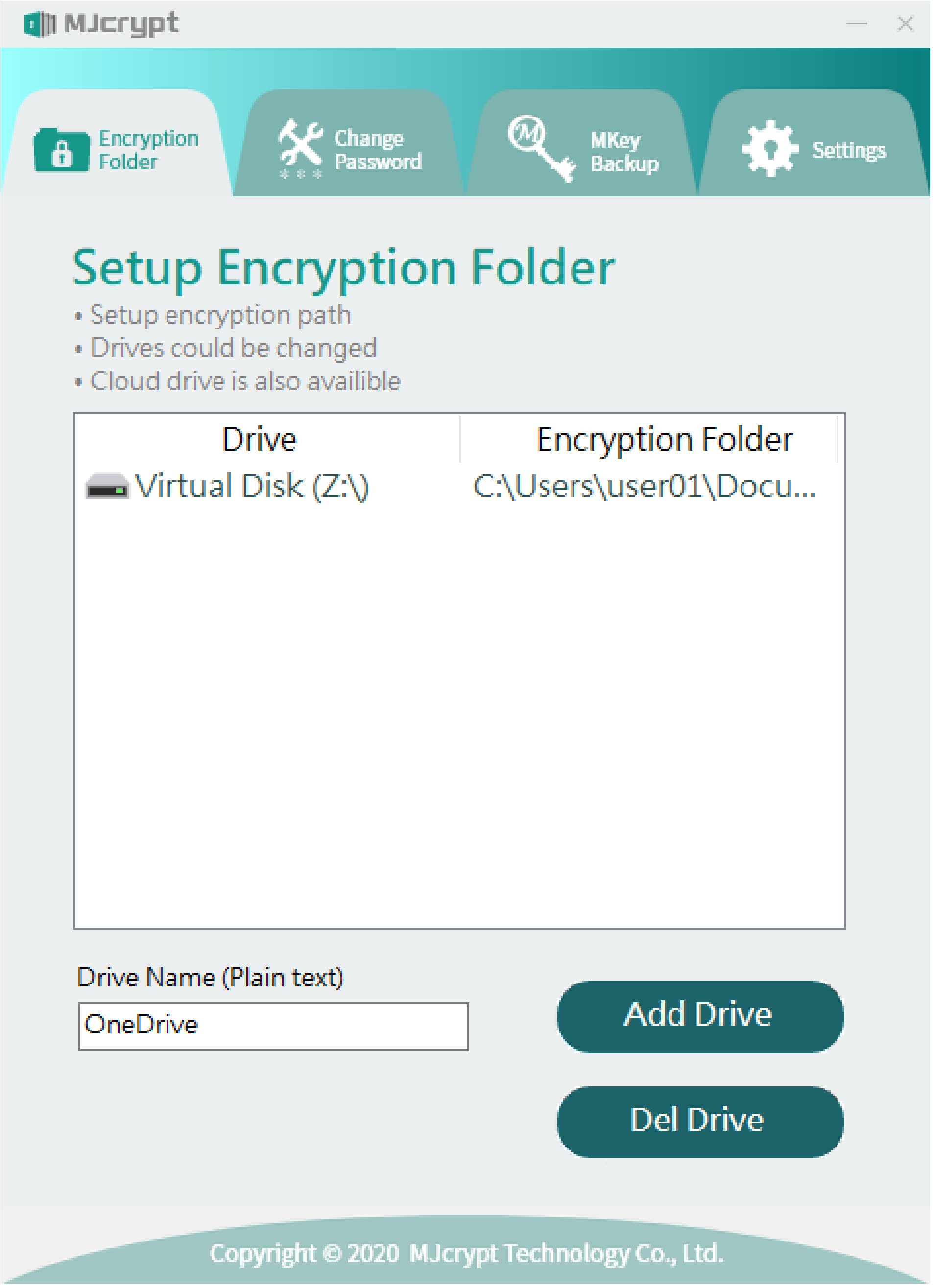
- Setup encryption path
- Drives could be changed
- Cloud drive is also availible

Drive	Encryption Folder
Virtual Disk (Z:\)	C:\Users\user01\Docu...

Double Click here shall open file explorer to plaintext virtual drive.

Double Click here shall open file explorer to Encryption Folder.

The following is the method of add a new mapping drive. Here we take the user setting “OneDrive” virtual disk mapping to the OneDrive synchronization directory area as an example. First, set the name of the virtual hard disk in the "Drive Name (Plain text)". The name is best to correspond to the user's purpose of use so that it can be easily found when the virtual disk is used, so setup “OneDrive” here. After setting the virtual disk name, click “Add Drive” .



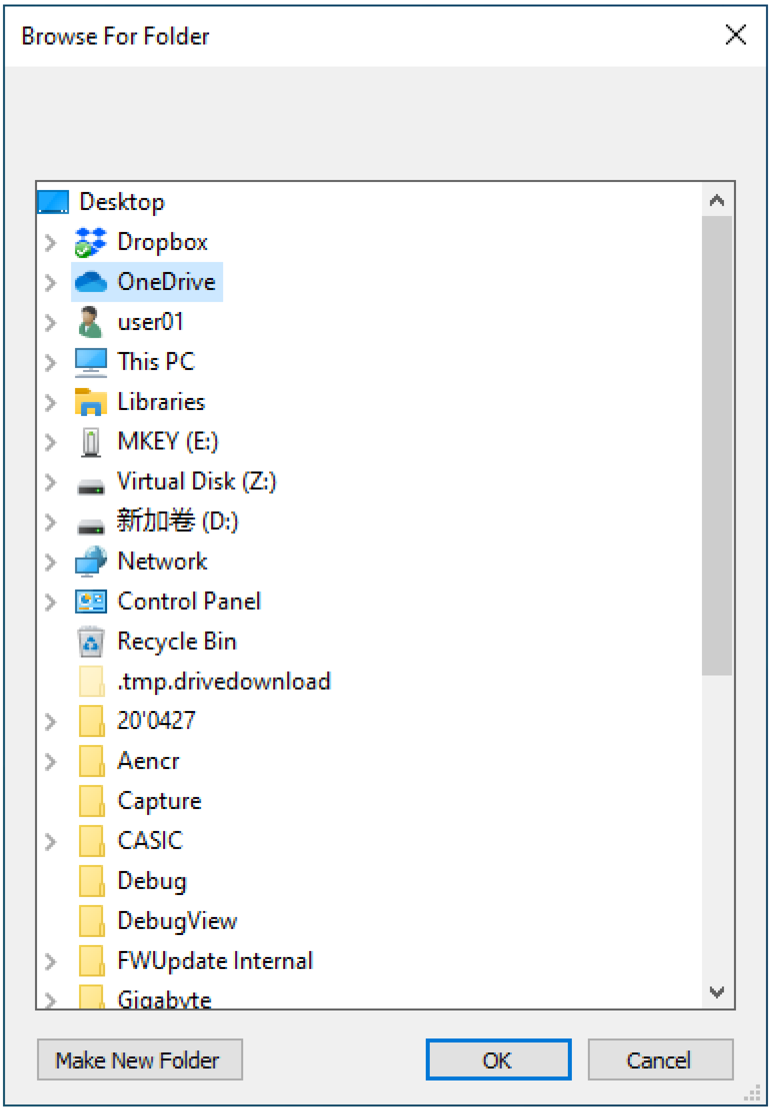
Setup Encryption Folder

- Setup encryption path
- Drives could be changed
- Cloud drive is also availible

Drive	Encryption Folder
Virtual Disk (Z:\)	C:\Users\user01\Docu...

Drive Name (Plain text): OneDrive

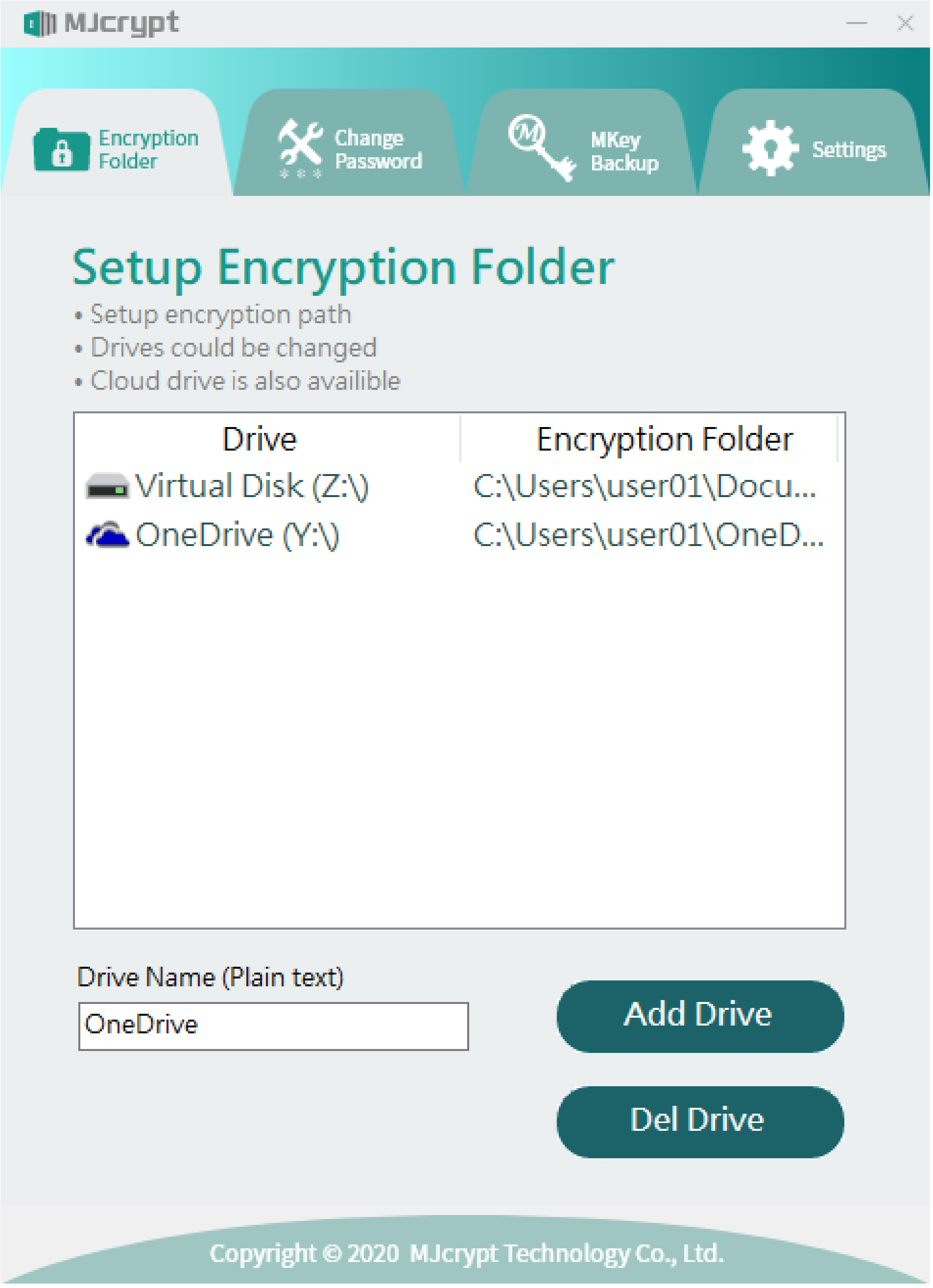
Then select a storage location for the encryption folder, the purpose is to set OneDrive folder for cloud disk synchronization, select it and press OK.



The setting of "Encryption Folder" has some restrictions. The following six areas cannot be set as the encryption folder of the encrypted file.

1. C: \ Program Files
2. C: \ Program Files (x86)
3. C: \ Program Data
4. C: \ Windows
5. Virtual disk
6. Encrypted area

The following figure is the result of adding a set of OneDrive corresponding. The virtual disk of the "Drive" corresponds to the "Encryption folder". The upper limit of the setting is six mapping setting, and the application will issue a warning when this limit is exceeded.



Setup Encryption Folder

- Setup encryption path
- Drives could be changed
- Cloud drive is also availible

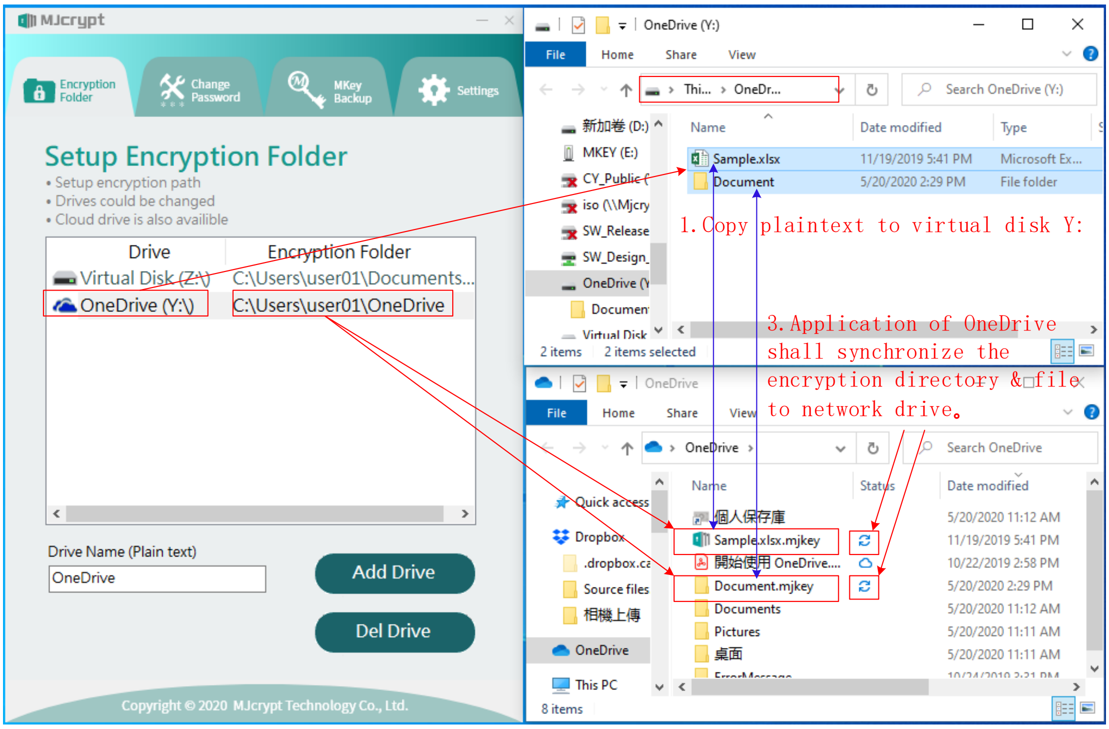
Drive	Encryption Folder
Virtual Disk (Z:\)	C:\Users\user01\Docu...
OneDrive (Y:\)	C:\Users\user01\OneD...

Drive Name (Plain text): OneDrive

If the user selects one of the corresponding locations of the virtual disk and presses the “Del Drive” button, the correspondence between the “Drive” and the “encrypted folder” will be released, but the files in the encryption folded will not be deleted.

If the data is copied to the virtual disk ‘Drive’ after the user has set it like step 1 below, the application program simultaneously generates encrypted files in the "Encryption Folder" at the same time, as shown in step 2 below. If the user has applied for an account of OneDrive and has logged in, the encrypted data will be synchronized to the OneDrive cloud disk through the OneDrive application, as in step 3 below.

If users have other Drive accounts, they only need to set the "Encryption Folder" to the Drive synchronization folder, and they can directly synchronize encrypted data with Drive. You can also use the same MKey to decrypt the uploaded encrypted data in other places (such as mobile phones).



Setup Encryption Folder

- Setup encryption path
- Drives could be changed
- Cloud drive is also availible

Drive	Encryption Folder
Virtual Disk (Z:\)	C:\Users\user01\Documents...
OneDrive (Y:\)	C:\Users\user01\OneDrive

Drive Name (Plain text): OneDrive

Name	Date modified	Type
Sample.xlsx	11/19/2019 5:41 PM	Microsoft Ex...
Document	5/20/2020 2:29 PM	File folder

1. Copy plaintext to virtual disk Y:

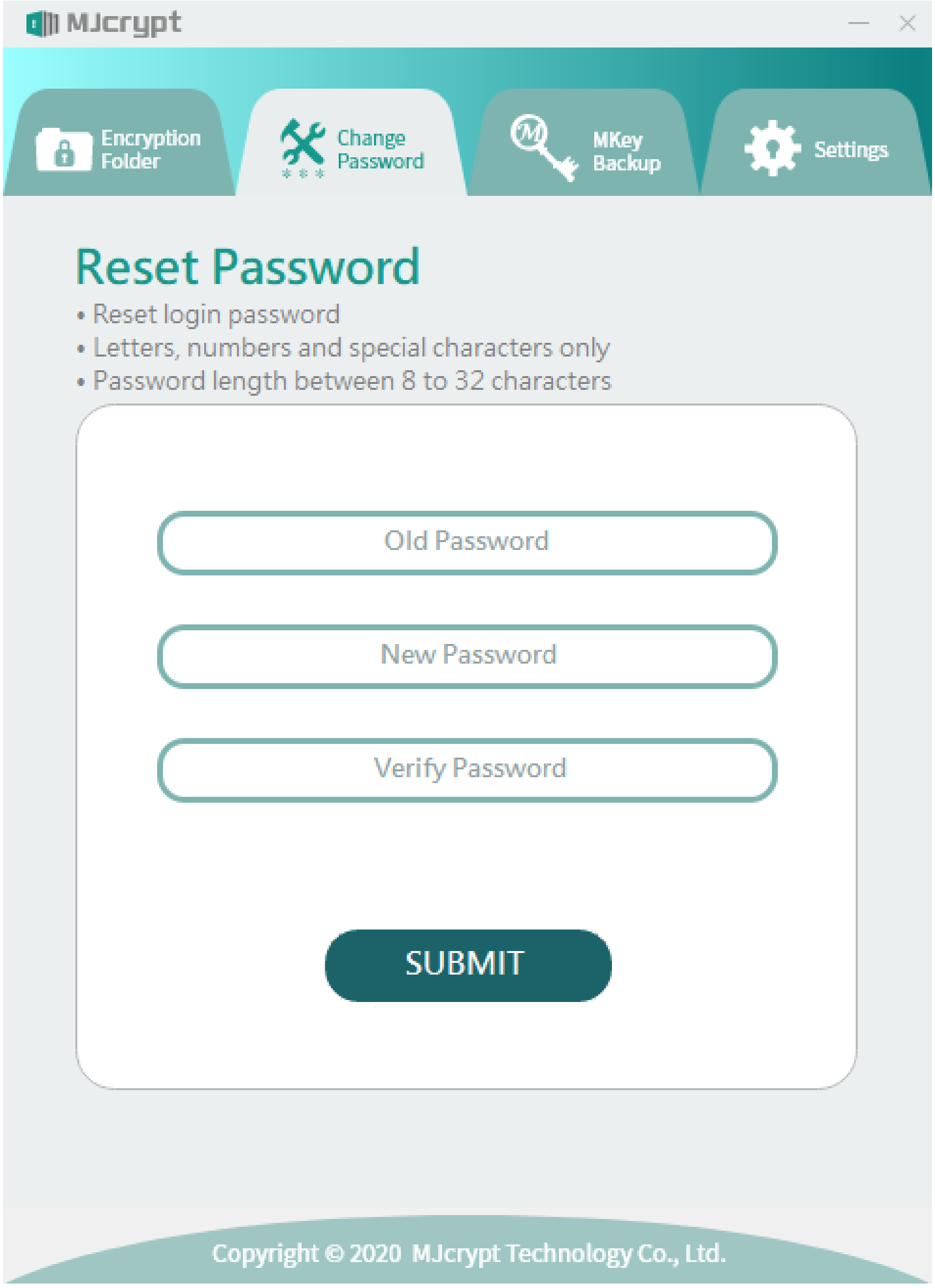
3. Application of OneDrive shall synchronize the encryption directory &file to network drive。

Name	Status	Date modified
個人保存庫		5/20/2020 11:12 AM
Sample.xlsx.mjkey		11/19/2019 5:41 PM
開始使用 OneDrive....		10/22/2019 2:58 PM
Document.mjkey		5/20/2020 2:29 PM
Documents		5/20/2020 11:12 AM
Pictures		5/20/2020 11:11 AM
桌面		5/20/2020 11:11 AM

2. Encryped directory & file are generated in “Encryption Folder”. Encrypted directory & file are with Filename extension “.mjkey”.

Change Password

The user must enter the current password in the “Old password” field and enter the same new password in the "New Password" and "Verify Password" fields. It is recommended that the user back up the key again after changing the password. The password setting length is limited to 8 ~ 32 characters.

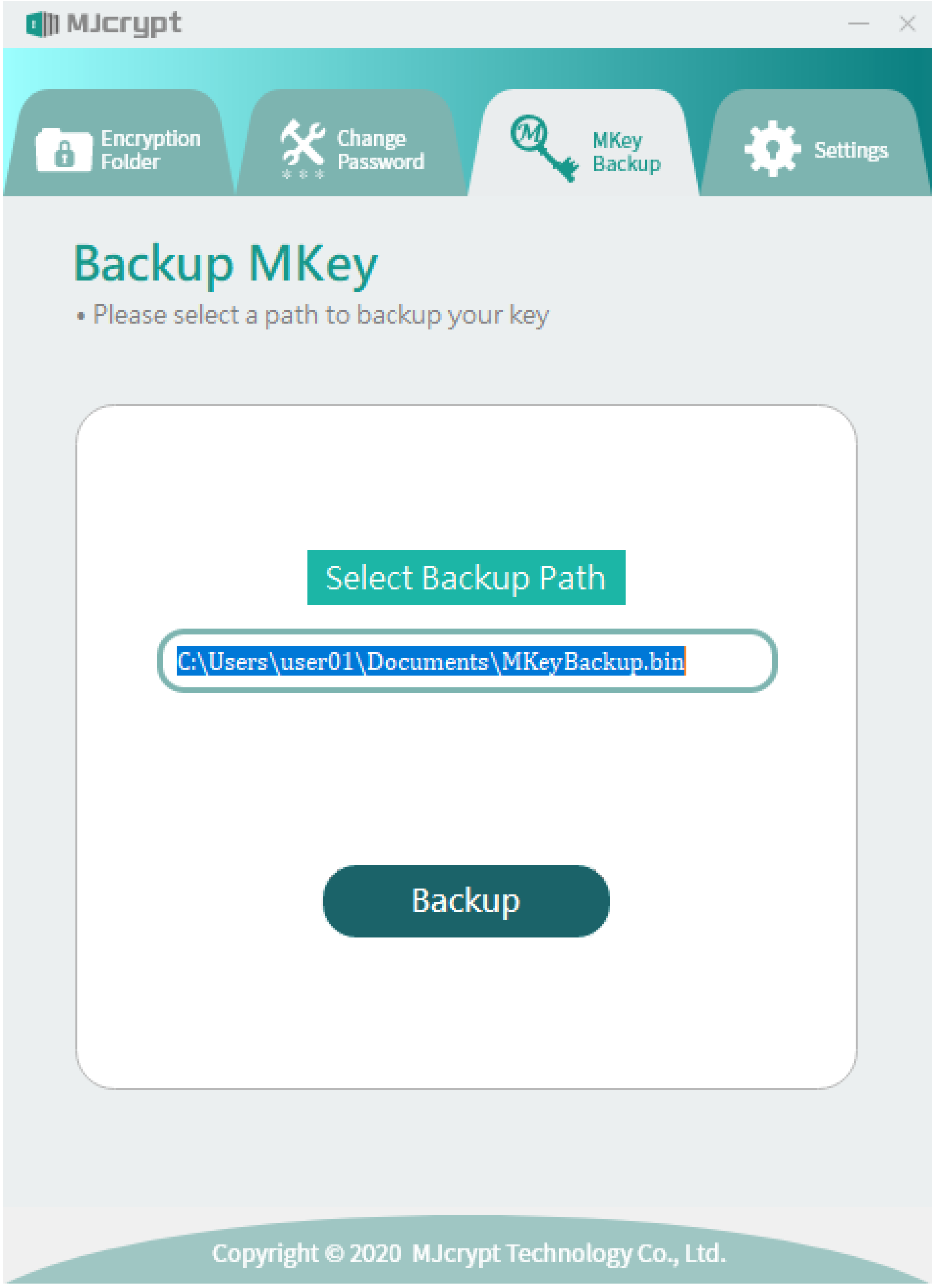


Reset Password

- Reset login password
- Letters, numbers and special characters only
- Password length between 8 to 32 characters

MKey Backup

The backup file of the key contains the password and the encryption/decryption key. These two kinds of information will be encrypted to generate a backup file. Please store it in a safe place in case the MKEY is accidentally damaged or lost. User can contact the MKey provider to use this backup file to create a new MKey for decrypting the original encrypted file. When the original factory makes a new MKey, the original key and password will be copied at the same time, allowing users to login using the password they originally set. The MKey provider cannot know the password set by the user during the process of duplicate a new MKey so that it ensure the security of user data. Therefore, users must never forget the password they set to prevent encrypted data from being decrypted.



Backup MKey

- Please select a path to backup your key

C:\Users\user01\Documents\MKeyBackup.bin

Copyright © 2020 MJcrypt Technology Co., Ltd.

Password: The data set by the user to login the software to use this application.

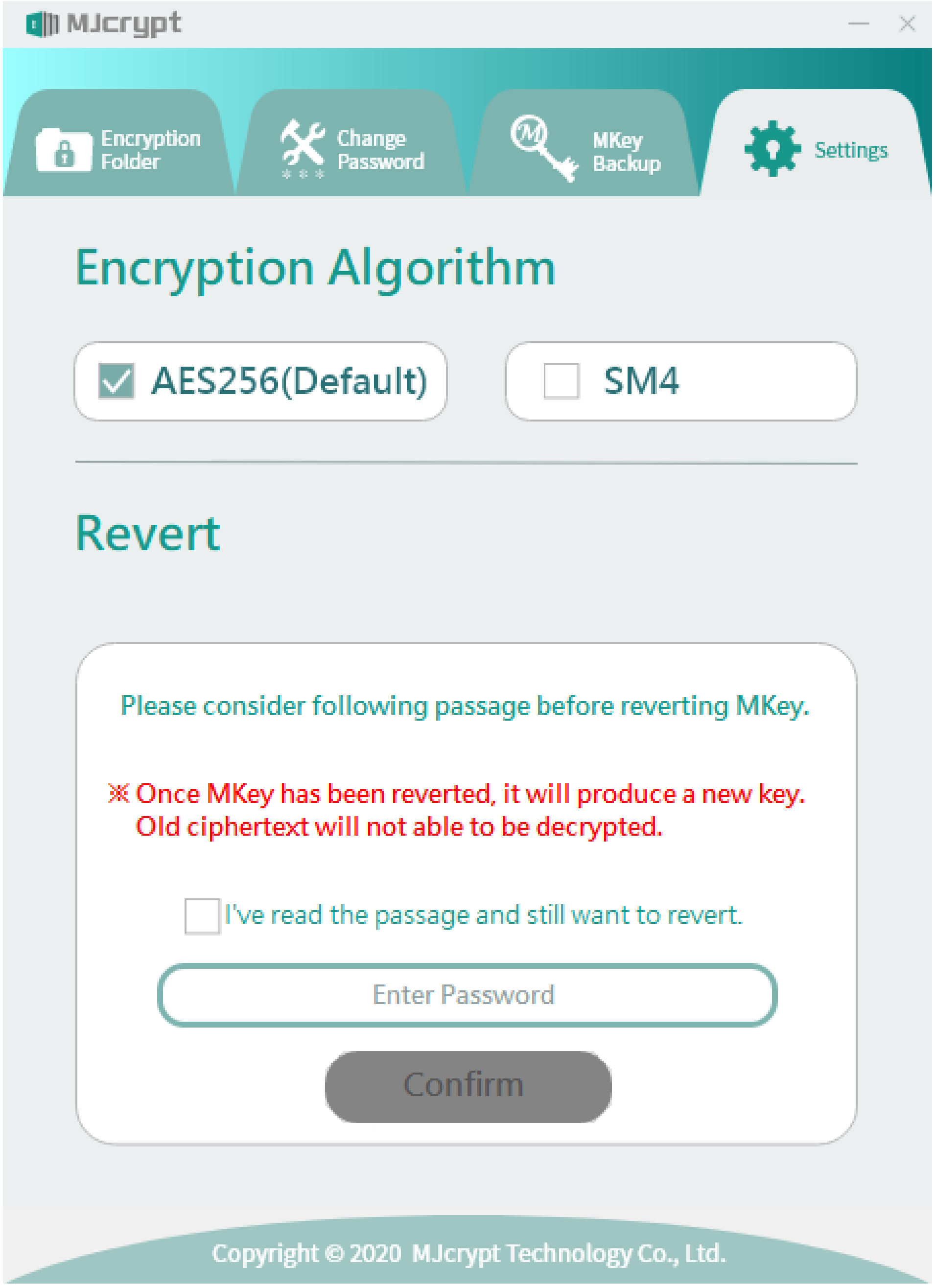
Encryption and decryption key: Random number is generated during production to encrypt and decrypt the data content. The Revert in the Settings will also make the encryption key to generate random numbers again.

Settings – Encryption Algorithm

There are two encryption methods for users.

AES256 - It’ s currently the most popular and secure encryption and decryption method in the world. This format same as the encryption and decryption of virtual disks.

SM4 - The encryption and decryption standard adopted by the People's Republic of China.



Encryption Algorithm

☑ AES256(Default) □ SM4

Revert

Please consider following passage before reverting MKey.

※ Once MKey has been reverted, it will produce a new key. Old ciphertext will not able to be decrypted.

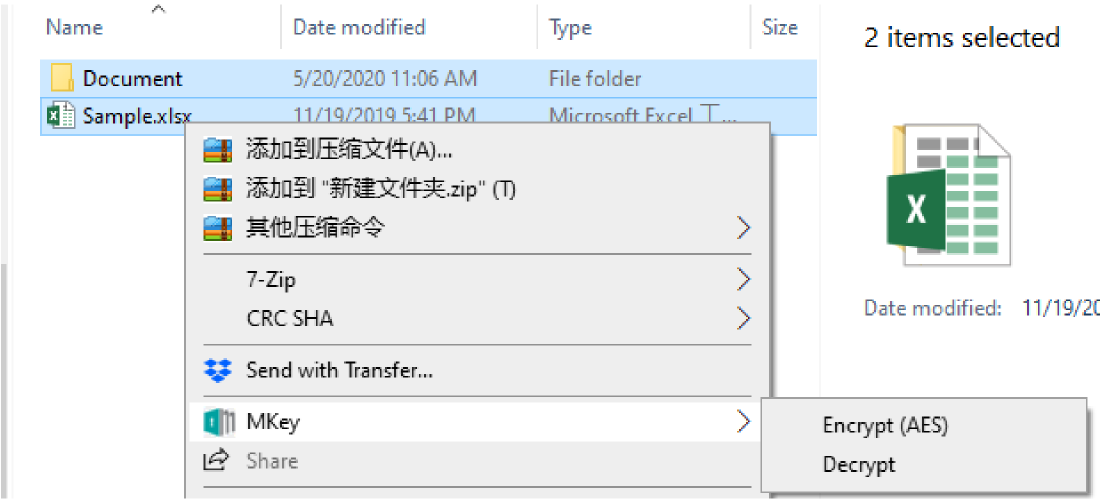
□ I've read the passage and still want to revert.

Enter Password

Confirm

Copyright © 2020 MJcrypt Technology Co., Ltd.

The usage of right key encryption and decryption is shown below. Move the mouse cursor to the file or directory that you want to encrypt and decrypt. You can select the files or directories for the function. Press the right mouse button and select encrypt or decrypt in MKey.



Settings – Revert

There are several purposes for user to revert MKey.

1. Use MKey first times. Let the key random number be generated again to ensure that unique MKey is created by yourself.
2. Give this MKey to others. To use files that you do not want others to have the opportunity to decrypt to encrypt you had ever used.
3. The encrypted data is scattered everywhere and is not easy to retrieve. User wants to quickly make the encrypted data unusable.

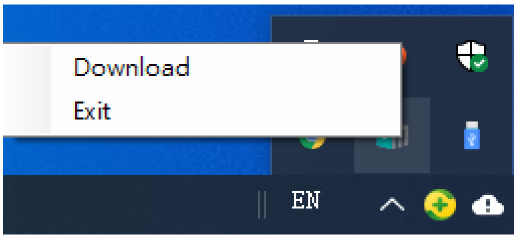
Please note that "Revert" does not allow the user to decrypt the encrypted data after the user forgets the password, so the password you set must never be forgotten.

Select the "I have read the message and still want to revert." Option and enter the correct password then press Confirm.

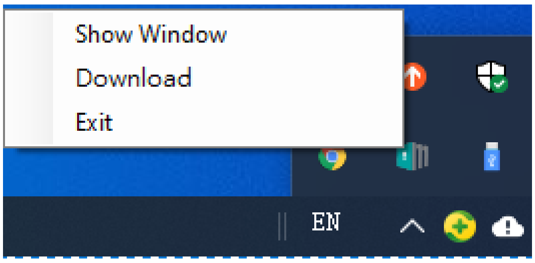
Hiding icons in the lower right corner

After the MKey application is installed, some functions of MKey are hidden in the lower right corner of Windows. It has different functions according to the status of MKey.

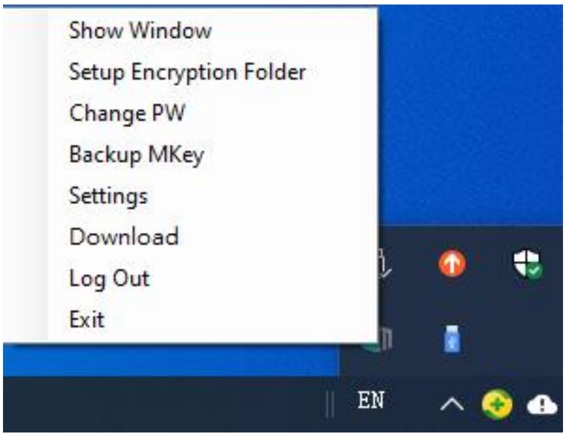
When MKey is not inserted



When not logging in when inserting MKey



After logging in when inserting MKey

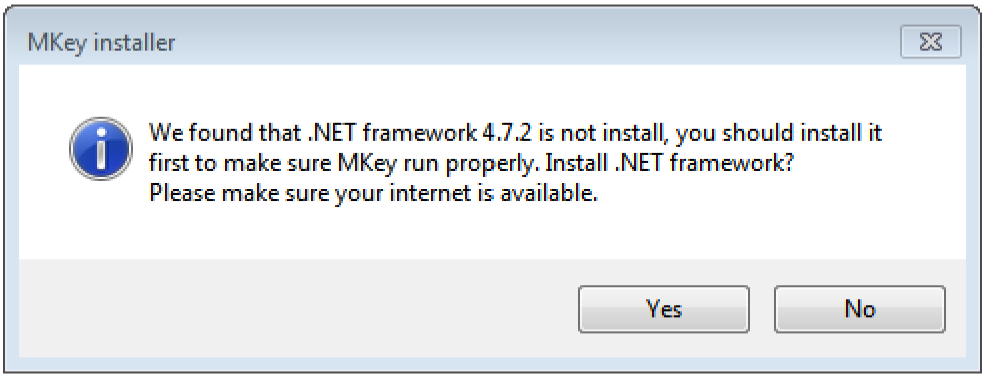


Selecting the corresponding project application will have the corresponding page display or function. In particular, the "Download" function is mentioned. Clicking this item will link to the newest download page of the latest data of MJcrypt Technology Corporation. https://www.mjcrypt.com/tw/download. Users can get the latest application information and Android applications here.

Common Problem

Windows Support

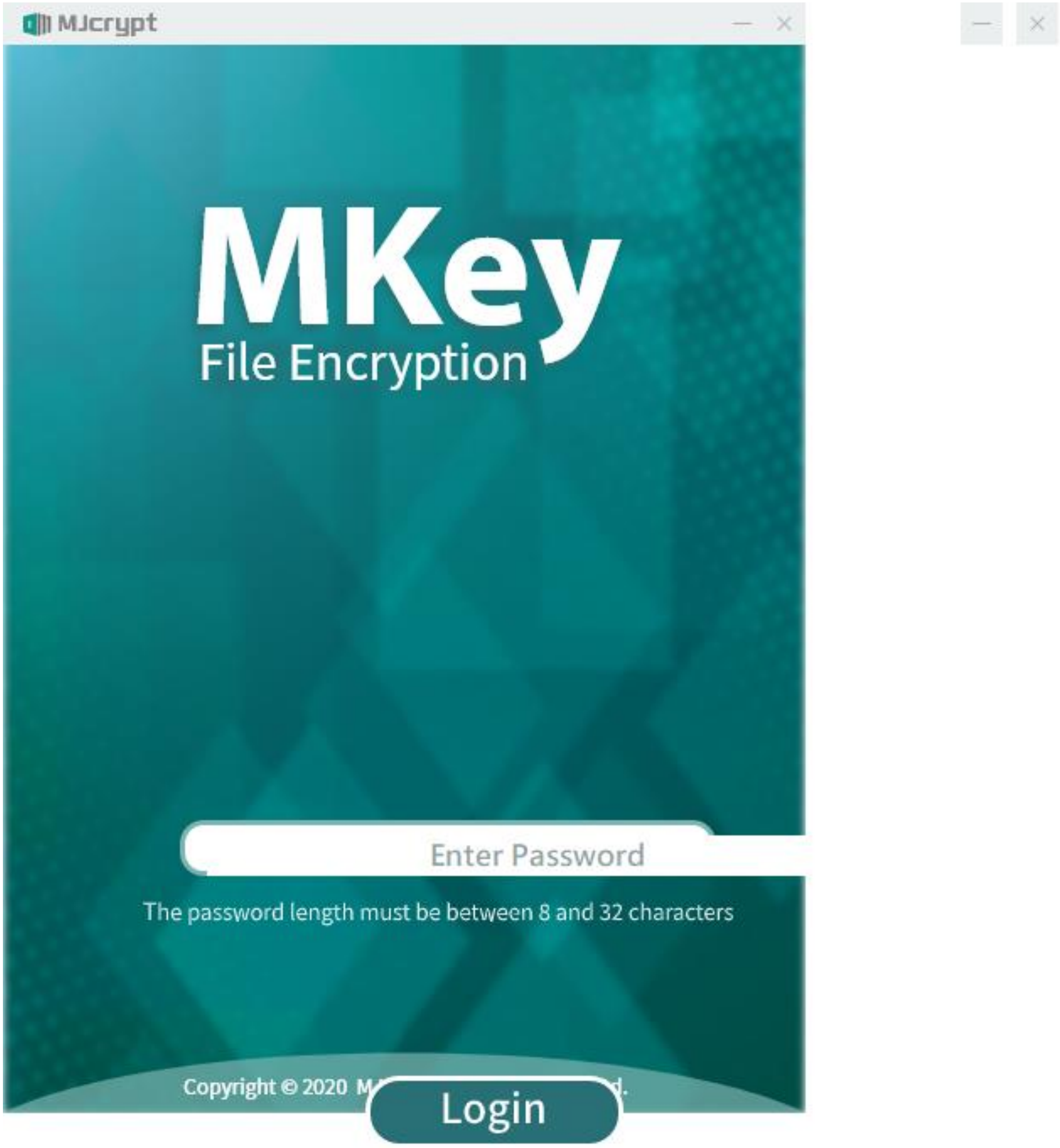
The application only supports Windows 7 and later versions. Windows 7 will be required to install .NET framework 4.7.2 before installation. Please install directly on the Internet. After the installation is complete, continue to install the MKey application.



We found that .NET framework 4.7.2 is not install, you should install it first to make sure MKey run properly. Install .NET framework?
Please make sure your internet is available.

Screen display problems

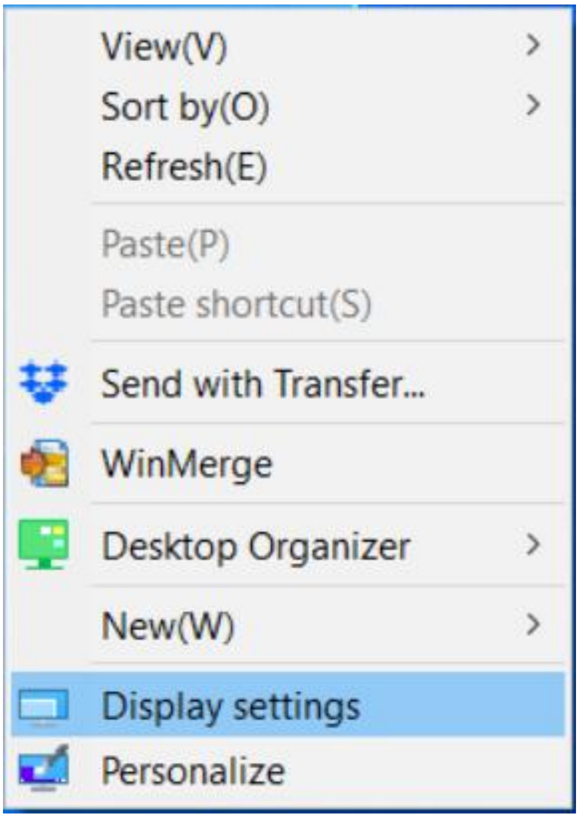
The user may encounter the problem of poor display of the following screen during use.



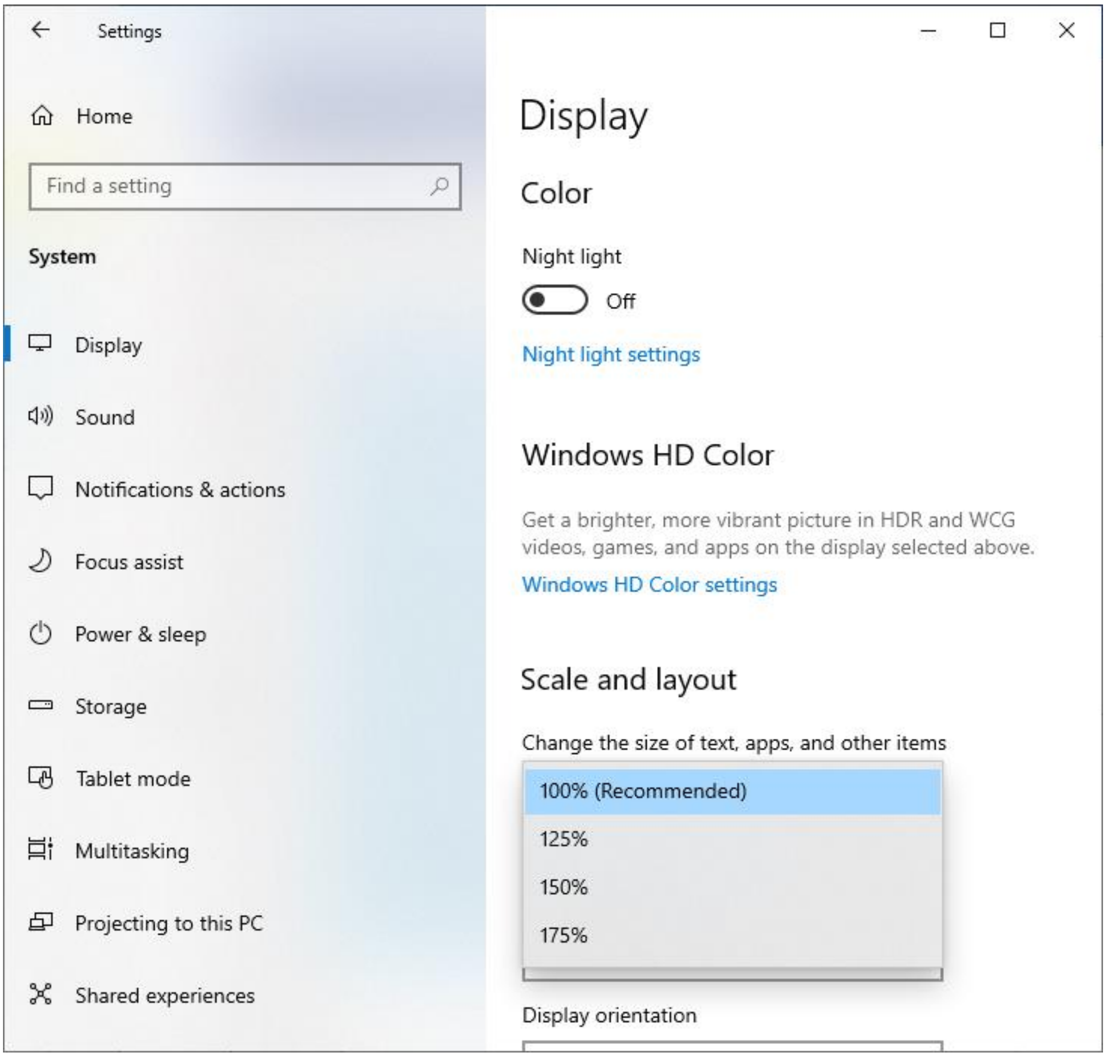
The password length must be between 8 and 32 characters

Please follow the procedure below to make corrections.

Move the mouse cursor to an empty space on the desktop and right-click to display the following screen.



The following screen appears after selecting the display settings



Display

Color

Night light

Off

Night light settings

Windows HD Color

Get a brighter, more vibrant picture in HDR and WCG videos, games, and apps on the display selected above.

Windows HD Color settings

Scale and layout

Change the size of text, apps, and other items

100% (Recommended)

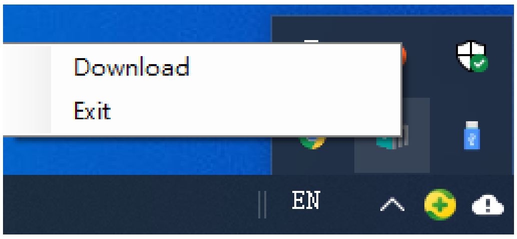
125%

150%

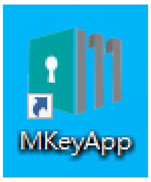
175%

Display orientation

Select 100% for changing text, size of application and other items.



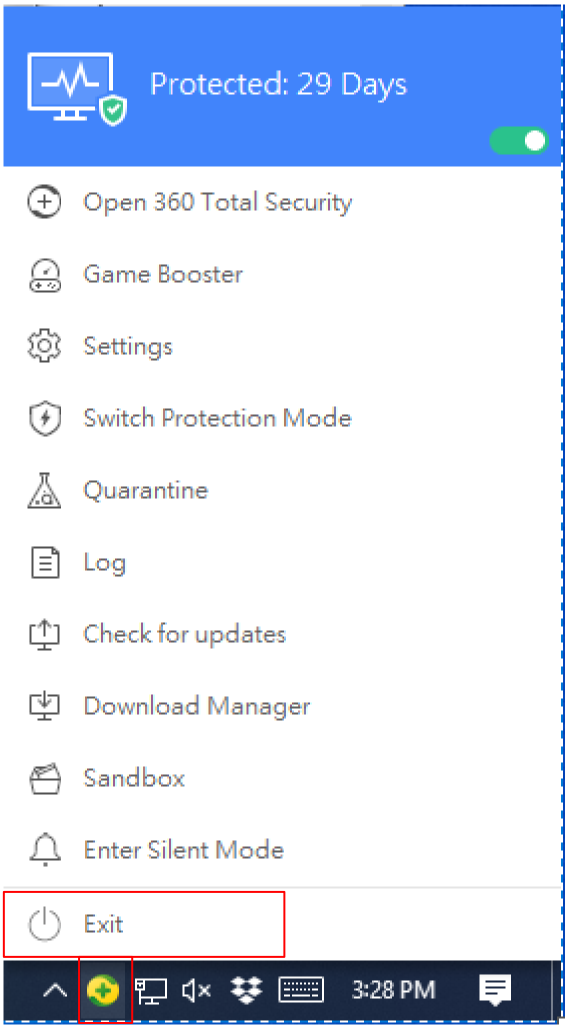
Please press exit in MKey hidden function.

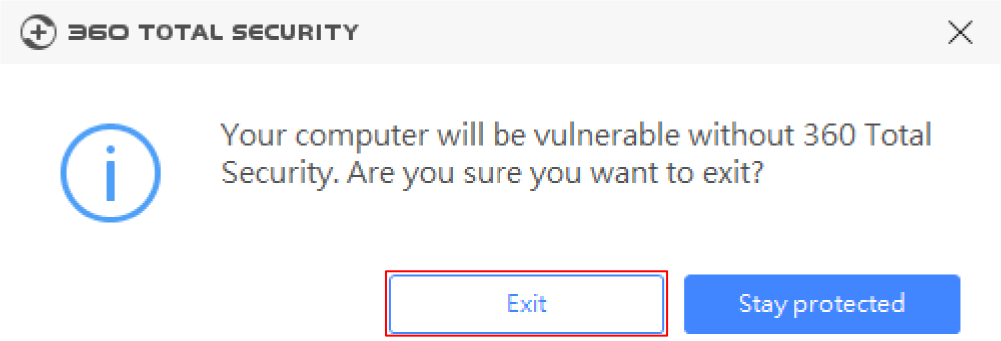


Double-click the MKeyApp icon on the desktop to restore the normal screen.

Problems with antivirus programs

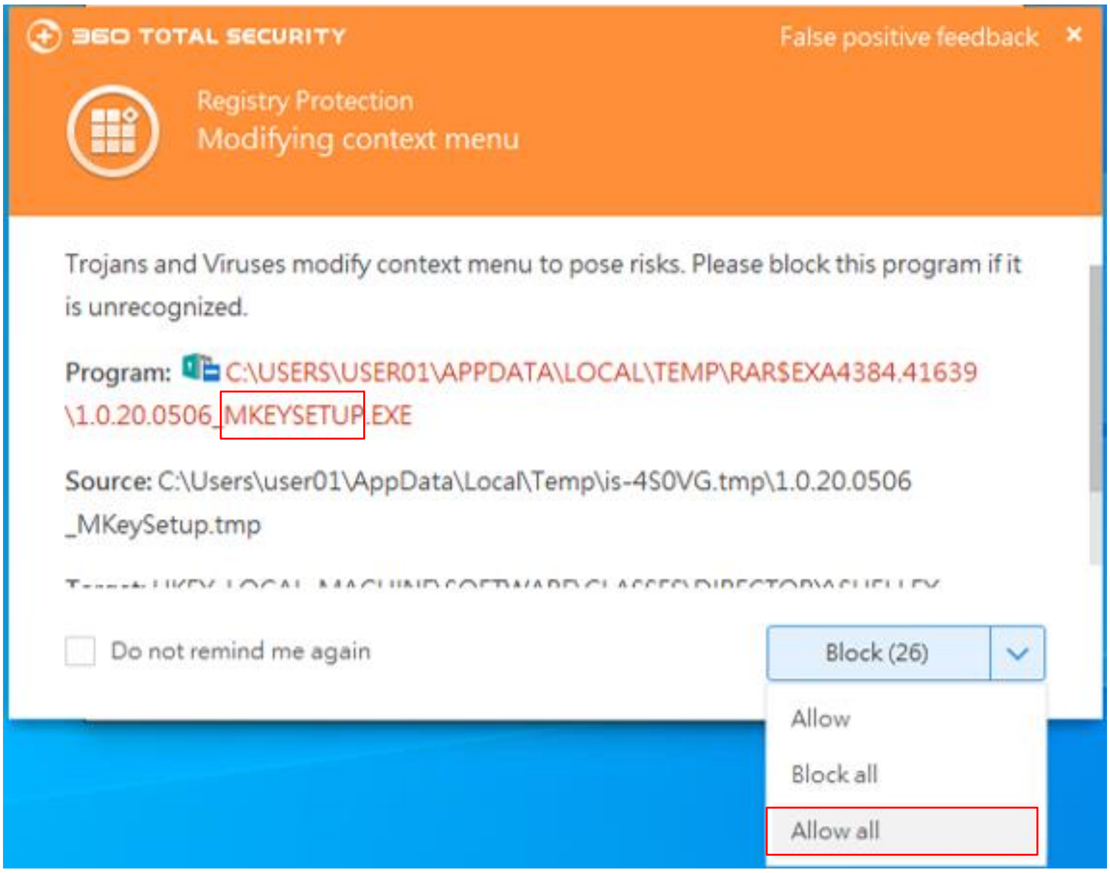
360 Total Security anti-virus software is the easiest to misjudge MKey anti-virus software, because it is often mistaken as a virus by 360 Total Security during the installation of MKey application. There are two ways to avoid it during installation. One is to temporarily stop the antivirus software. Open the hidden window from the 360 total security icon in the lower right corner, press “Exit” to temporarily stop the 360 Total security and then open it after the installation is completed.




360 TOTAL SECURITY

Your computer will be vulnerable without 360 Total Security. Are you sure you want to exit?

The second is to install the MKey installer directly and wait for the pop-up warning window of 360 Total Security to deal with it. If any programs with MKeySetup string, installation path (usually C: \ Program Files \ MKEY) and donkon1.sys are found to be intercepted by 360 total security, please choose “Allow all” selection item.


360 TOTAL SECURITY

Registry Protection

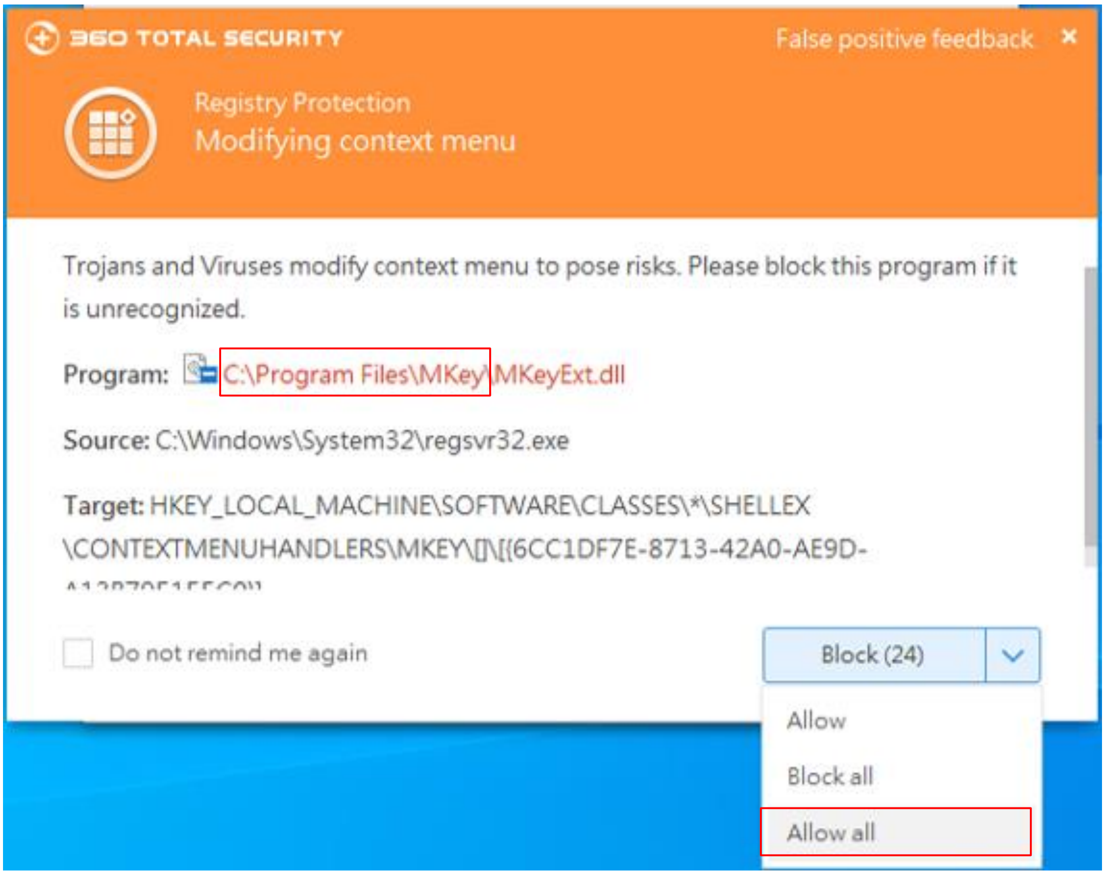
Modifying context menu

Trojans and Viruses modify context menu to pose risks. Please block this program if it is unrecognized.

Program: C:\USERS\USER01\APPDATA\LOCAL\TEMP\RAR$EXA4384.41639\1.0.20.0506_MKEYSETUP.EXE

Source: C:\Users\user01\AppData\Local\Temp\is-4S0VG.tmp\1.0.20.0506_MKeySetup.tmp

Target: HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\DIRECTORY\SHELLEX



Registry Protection
Modifying context menu

Trojans and Viruses modify context menu to pose risks. Please block this program if it is unrecognized.

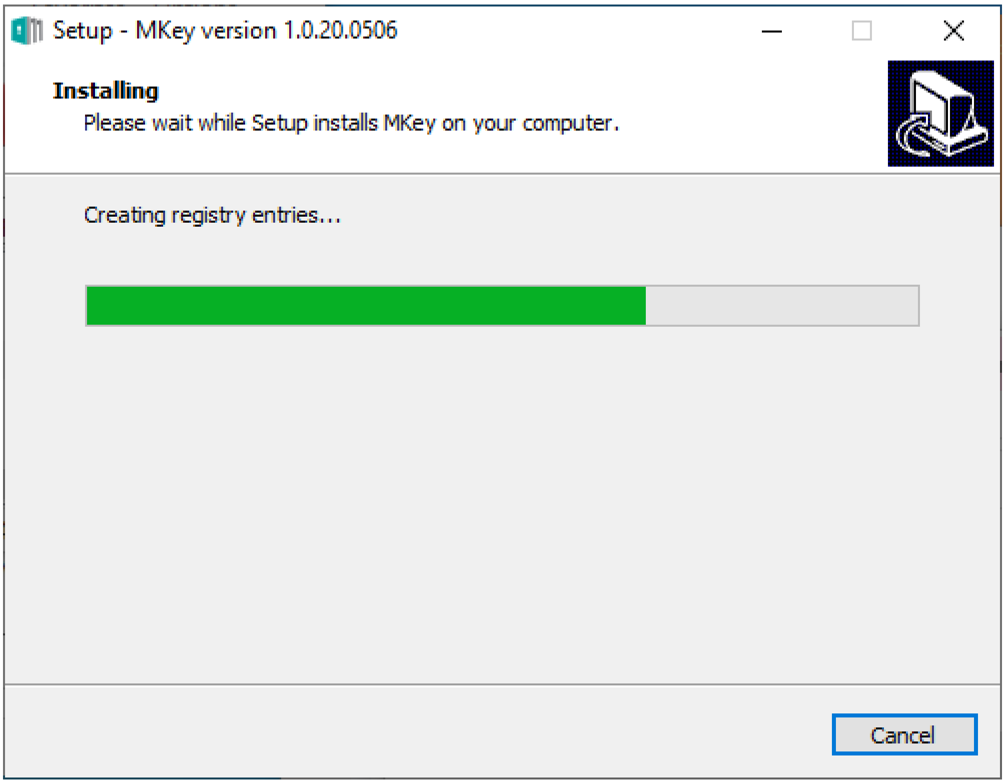
Program: C:\Program Files\MKey\MKeyExt.dll

Source: C:\Windows\System32\regsvr32.exe

Target: HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\*\SHELLEX\CONTEXTMENUHANDLERS\MKEY\[]\[{6CC1DF7E-8713-42A0-AE9D-

□ Do not remind me again

The installation process of the MKey application should be smooth all the way. If you encounter a pause of more than 10 seconds to the middle of the installation (as shown below), the window representing 360 Total Security may be covered by this installation window. Please click on the 360 Total Security Guard Window "Allows all" selection.



Setup - MKey version 1.0.20.0506

Installing

Please wait while Setup installs MKey on your computer.

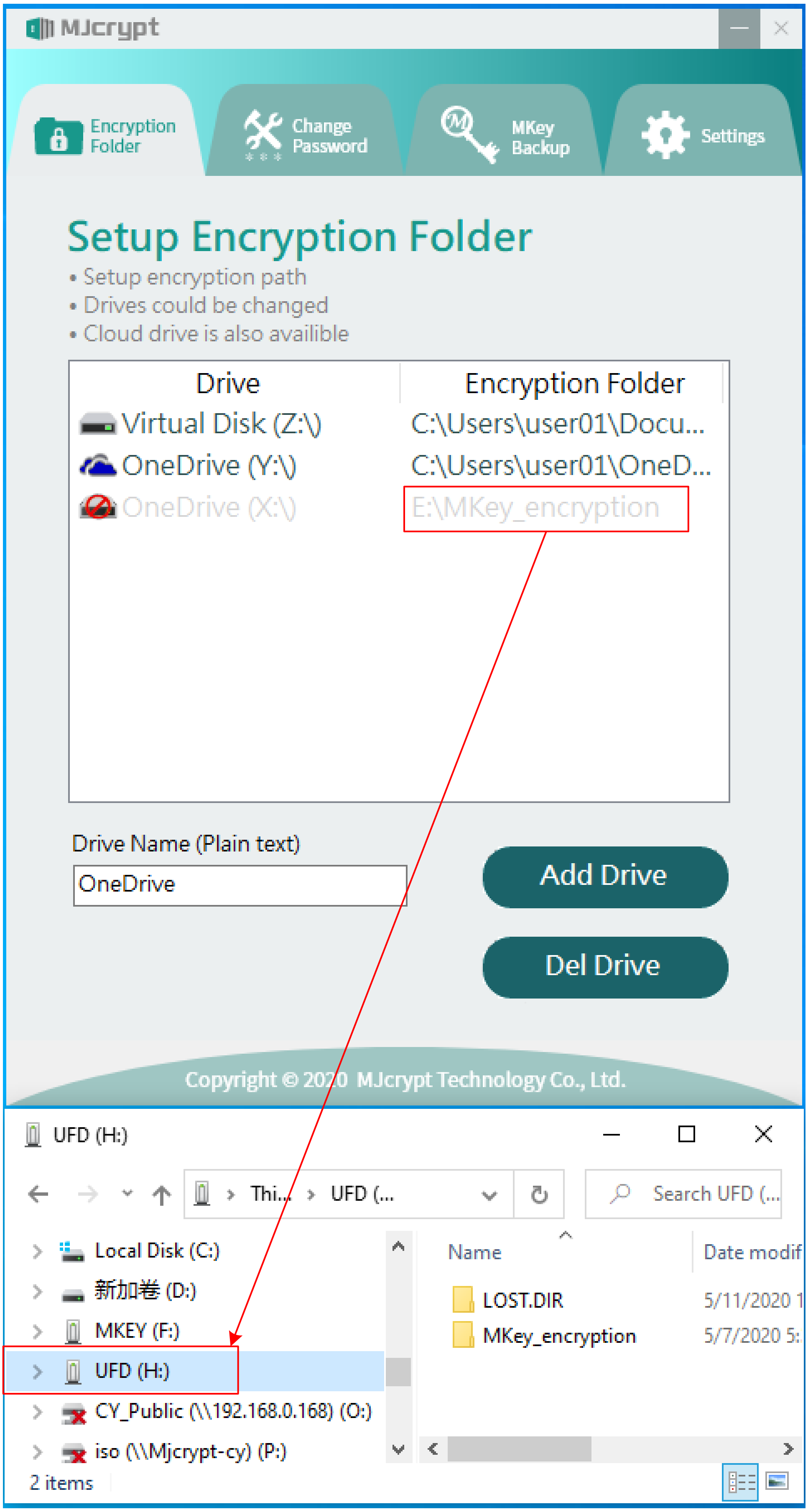
Creating registry entries...

The Encryption Folder disappears

If the user uses an USB portable disk as encryption folder, it is feasible. However, because the user may insert multiple USB portable disk or just insert only one USB portable disk in different using purpose, the drive number of the **mapping USB portable disk** may be changed by the operating system if user plug **other non-mapping USB portable disks** then plug **mapping USB portable disk**. As a result, the using drive encryption folder is different from the originally encryption folder in drive number. As shown in the figure below, the original encryption folder is at E: because of the insertion of **2 other USB portable disks**, then plug in the **mapping USB portable disk** the drives is changed to H: by the operating system. The original setting encryption folder cannot be found in the original drive. The APP will display that the setting does not exist to remind the user that there is a mapping problem with the setting.

There are two ways for users to troubleshoot problems.

1. Remove the original encryption folder (E: \ MKey_Encryption) and re-set it to a new encryption folder (H: \MKey_encryption). This change will only change the Drive & Encryption Folder mapping relation and will not affect the data content.
2. Temporarily remove the **other non-mapping portable USB disks** and re-plug in the **mapping USB portable disk** to make the encryption folder is back to (E: \ MKey_Encryption).



Setup Encryption Folder

- Setup encryption path
- Drives could be changed
- Cloud drive is also availible

Drive	Encryption Folder
Virtual Disk (Z:\)	C:\Users\user01\Docu...
OneDrive (Y:\)	C:\Users\user01\OneD...
OneDrive (X:\)	E:\MKey_encryption

Drive Name (Plain text): OneDrive

Copyright © 2020 MJcrypt Technology Co., Ltd.

Name	Date modif
LOST.DIR	5/11/2020 1
MKey_encryption	5/7/2020 5:

2 items