

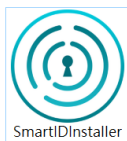
Smart ID User Manual

Thank you for using the Smart ID product. This user manual will guide you to adventure the wonderful features of the product.

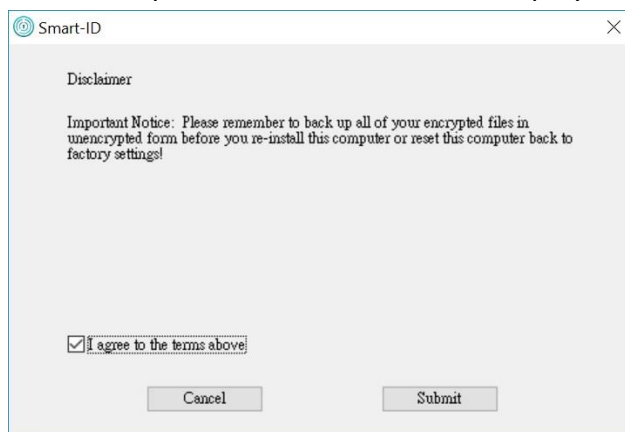
1. How to install Smart ID software

Insert the Smart ID dongle.

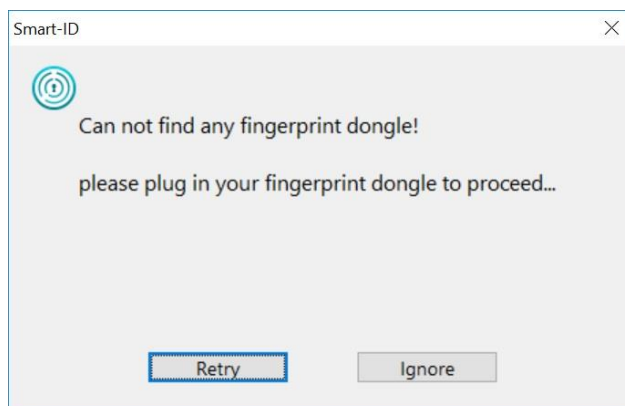
Get the SmartIDInstaller software. Double click the execution file.



Follow the process of the installation step by step.



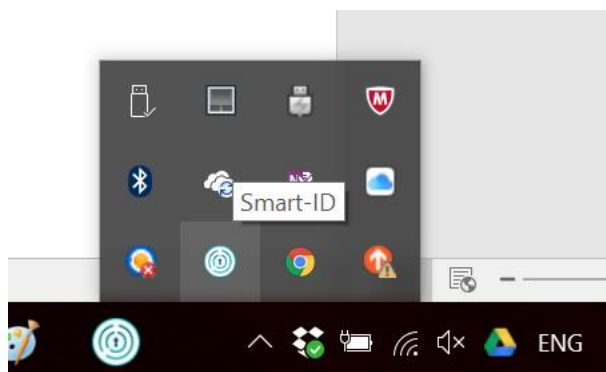
If you did not plug in the dongle, the following message will pop up. However, you can choose "Ignore" to proceed.



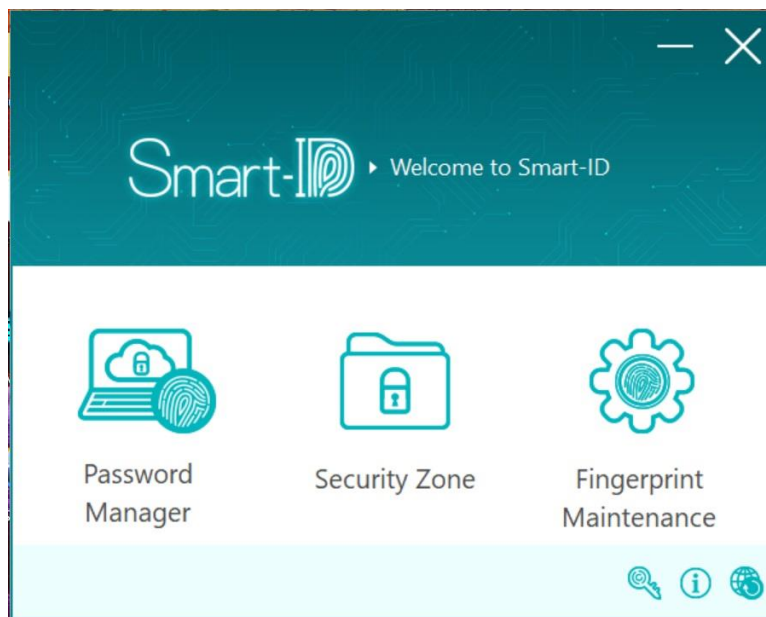
After installation, the Smart-ID program will be launched. Also, you can find the program link on desktop.



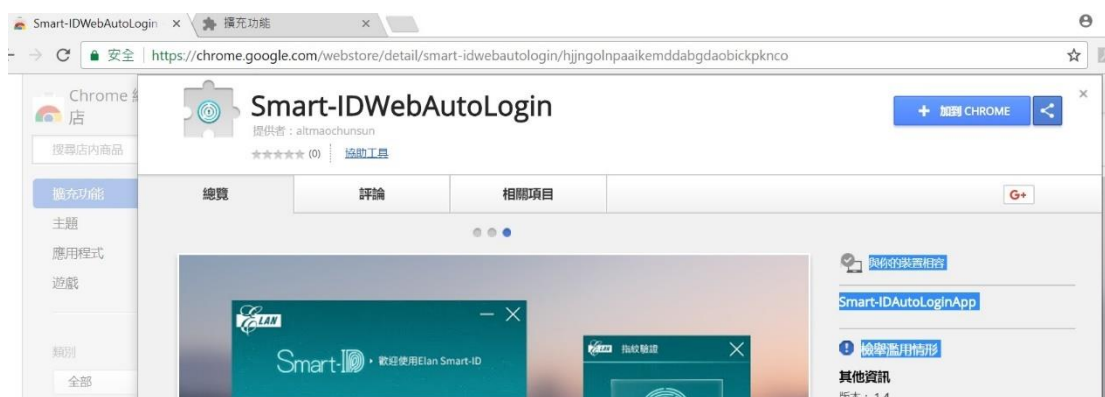
You can also find the program in the shortcut area after the program executed.



Main panel of the program.



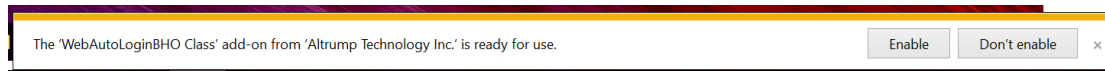
If you have Chrome installed, the following Smart-IDWebAutoLogin program should be install.



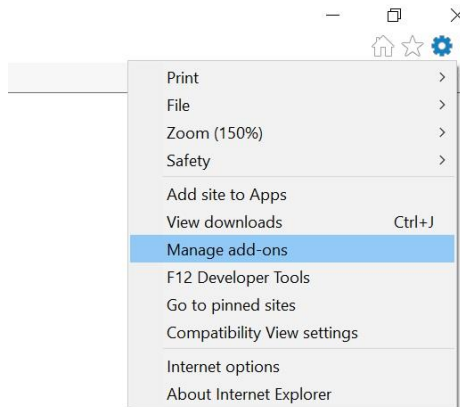
Please install and enable the addon program.



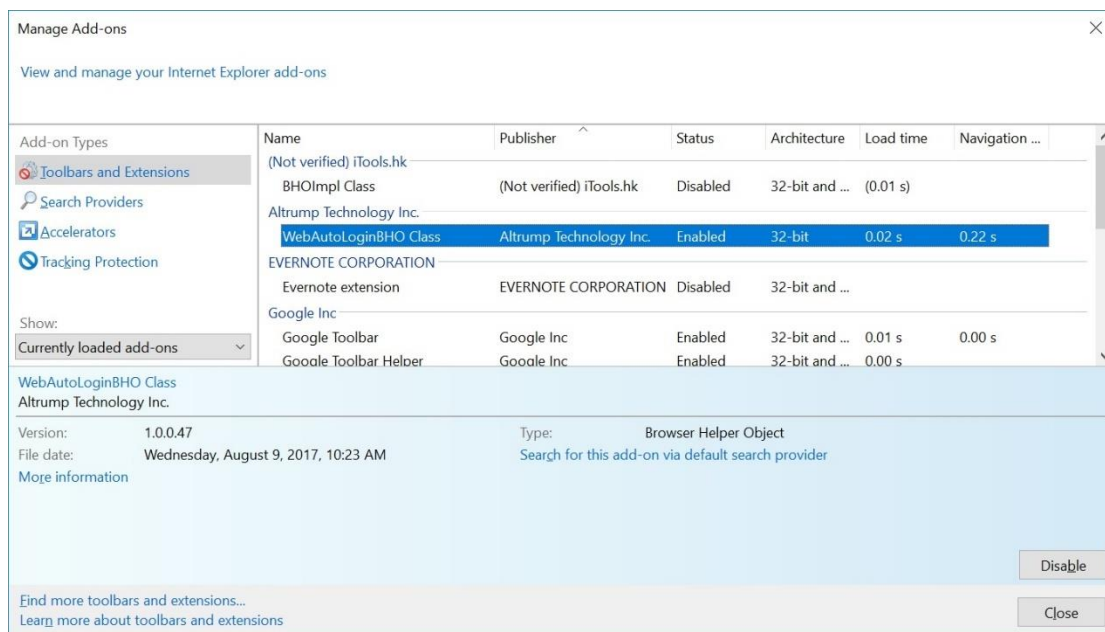
Attention: when the IE browser launched first time after installation, the following message will pop up. Please choose “enable”.



Or, you can check the “Manage add-ons” by clicking the setting icon of IE.

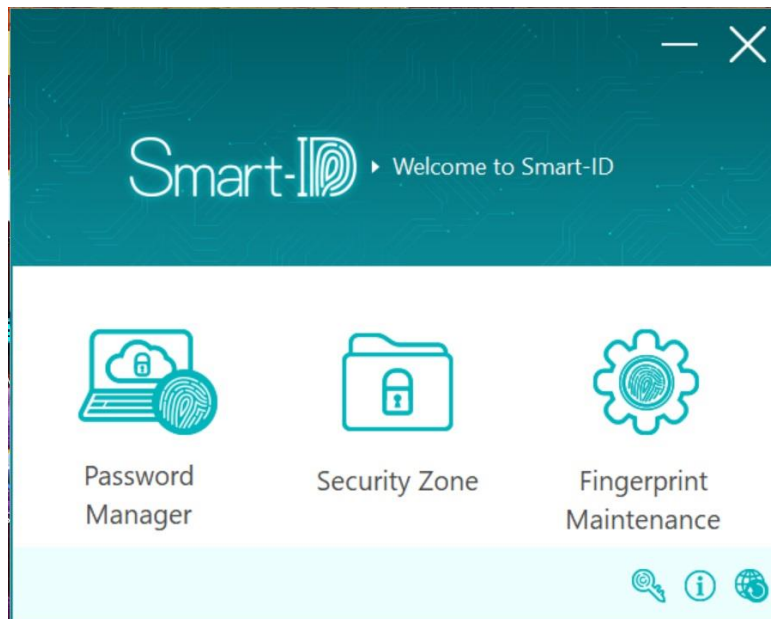


Please make sure the WebAutoLoginBHO program has been activated.

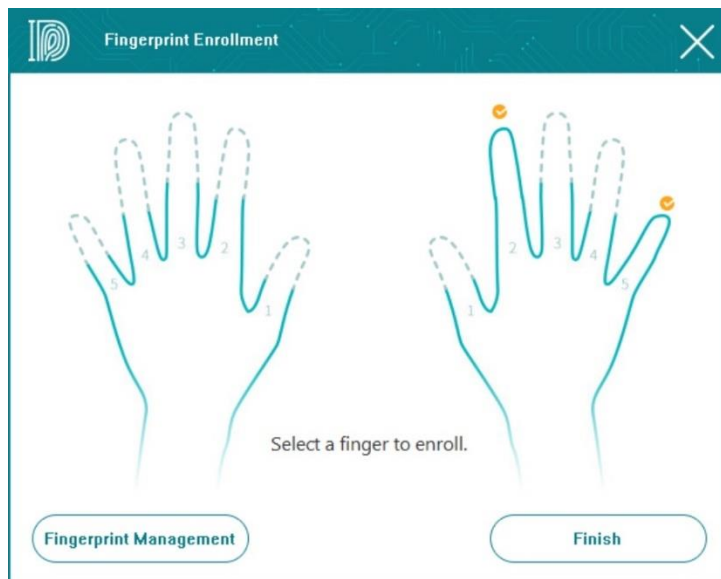


2. How to enroll your fingerprint

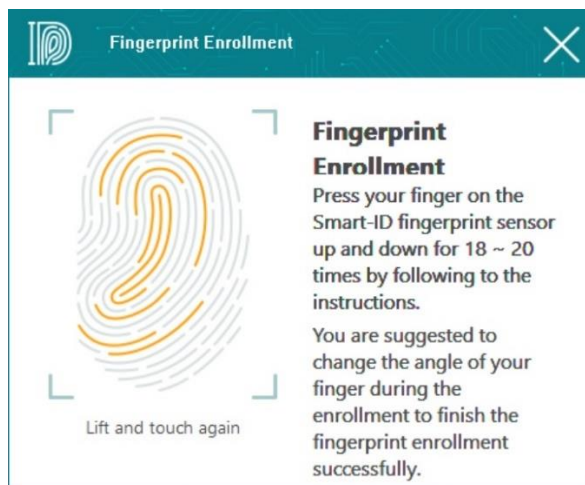
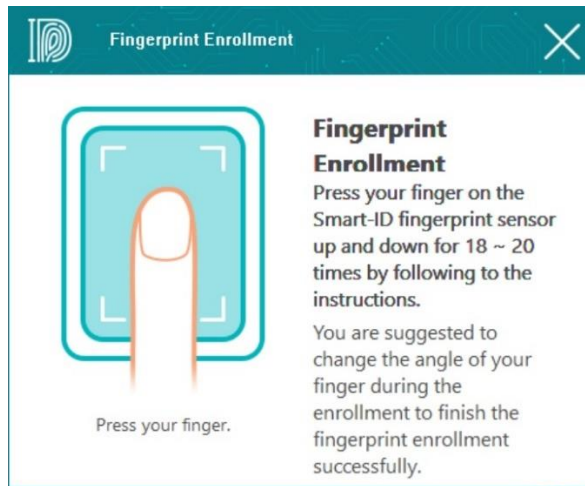
Click the “Fingerprint Maintenance” function on the main panel.



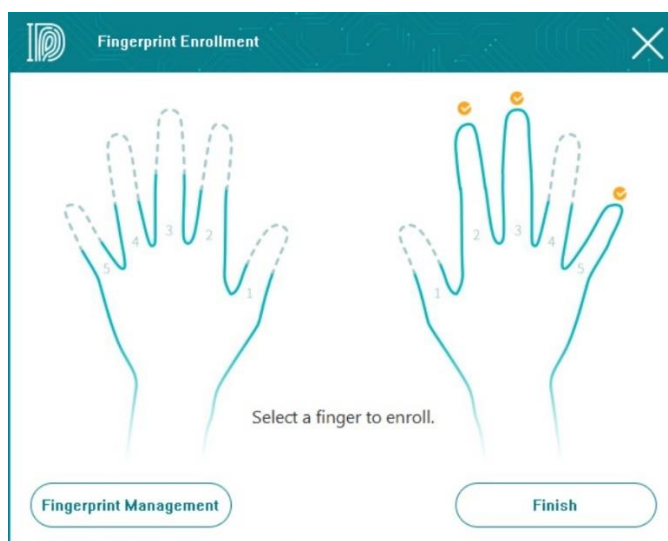
Choose which finger you will enroll. For example, the middle finger.



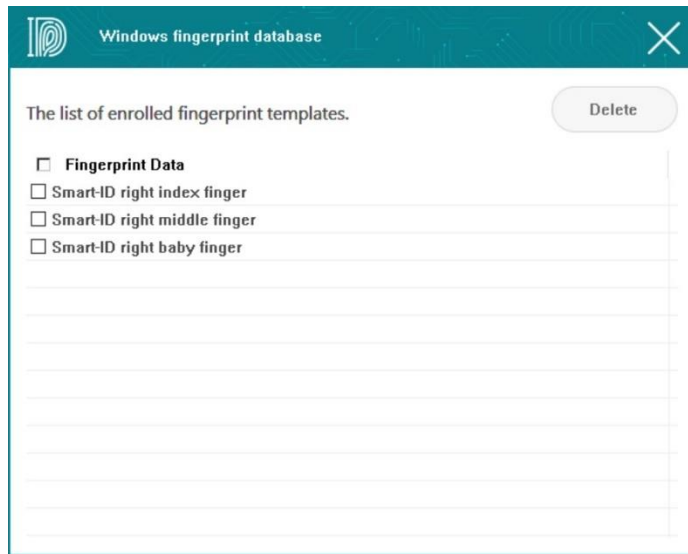
Follow the instruction on the screen.



After finishing, the finger you enrolled will be check.

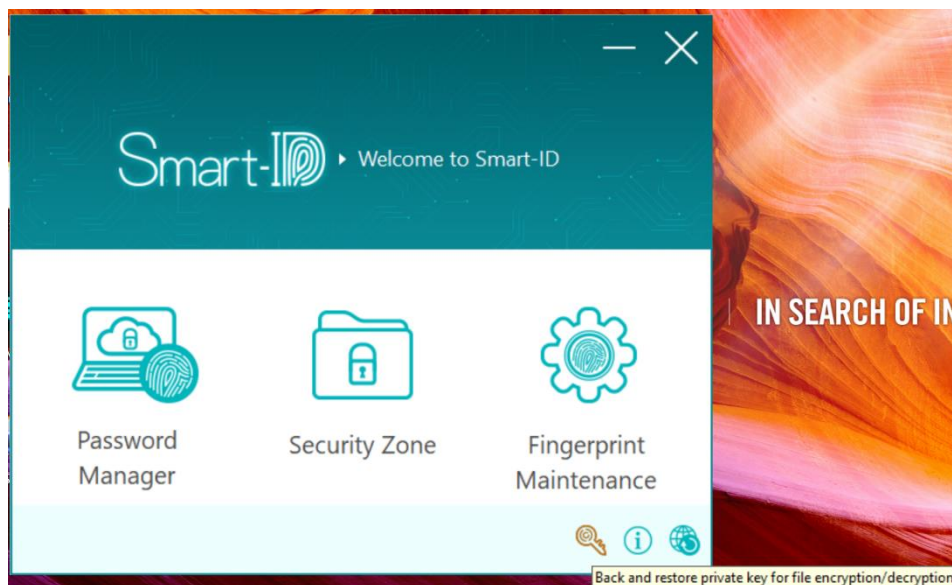


You can check the list of the fingerprint database by clicking the “Fingerprint Management function on the Fingerprint Enrollment window.

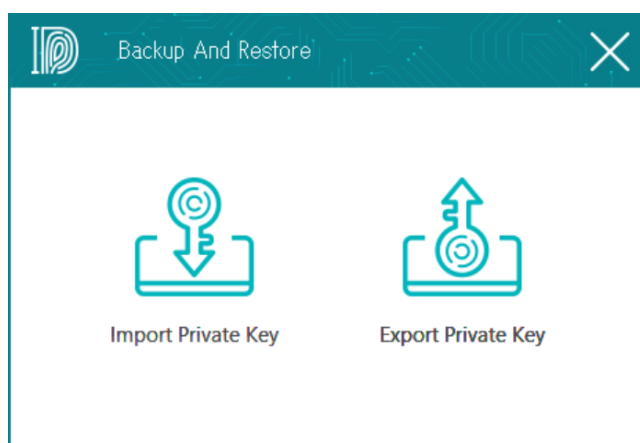


3. Backup and Restore Private Key

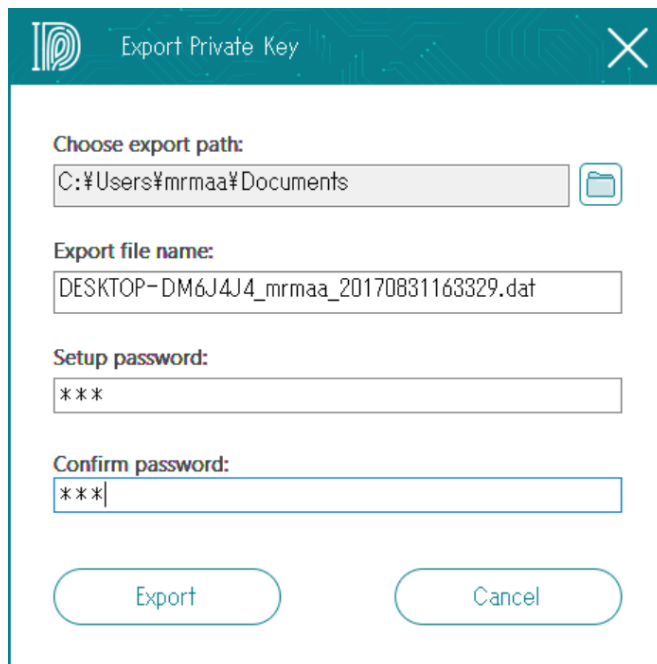
A private key is a random string of bits created explicitly for scrambling and unscrambling data. Private keys are designed with algorithms intended to ensure that every key is unpredictable and unique. Once Smart-ID been installed or reinstalling Windows, a new private key will automatically be generated. Strongly recommend that user backup the private key when installing Smart-ID. It will prevent the private key mismatching from reinstalling Windows.



First, click the “key” icon on the right down corner. The following “Backup And Restore” window will be popped up.



Export private key: Please select “Export Private key” to back up.



The dialog box titled "Export Private Key" has a teal header with a fingerprint icon and a close button. It contains four input fields: "Choose export path:" with the text "C:\Users\mrmaa\Documents" and a folder icon; "Export file name:" with the text "DESKTOP-DM6J4J4_mrmaa_20170831163329.dat"; "Setup password:" with three asterisks; and "Confirm password:" with three asterisks. At the bottom are "Export" and "Cancel" buttons.

Export Private Key

Choose export path:
C:\Users\mrmaa\Documents

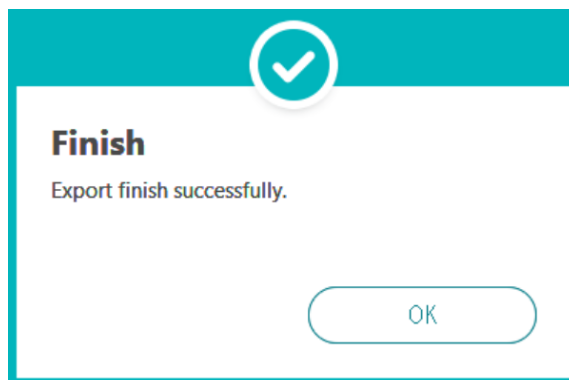
Export file name:
DESKTOP-DM6J4J4_mrmaa_20170831163329.dat

Setup password:

Confirm password:

Export Cancel

Select the path where to store the private key. Enter the file name or you can use the default one. Set the password to protect the private key.



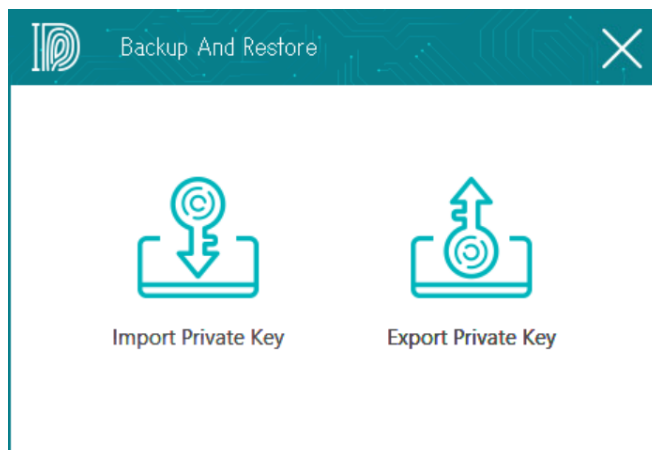
The dialog box titled "Finish" has a teal header with a white checkmark icon. It contains the text "Export finish successfully." and an "OK" button at the bottom.

Finish

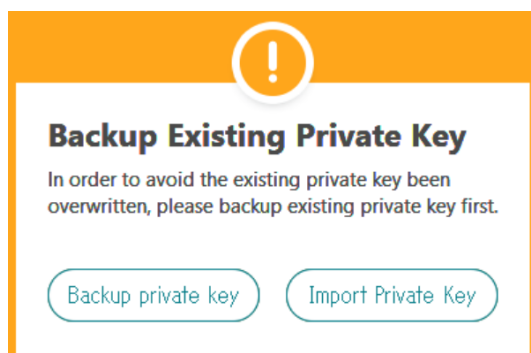
Export finish successfully.

OK

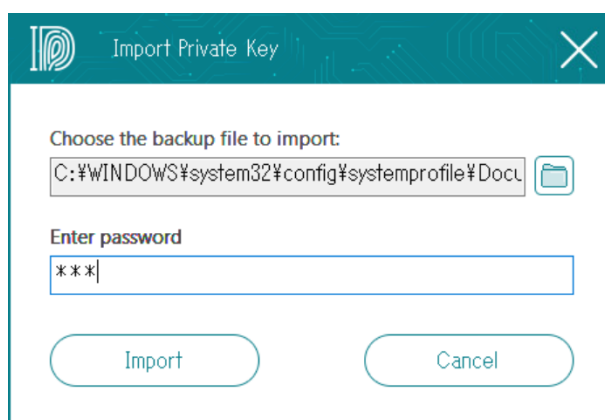
Import private key: Please select “Import Private key” to restore.



Note: Restore private key will overwrite the existing private key. If you had already encrypted files, please backup the existing private key before restoring.

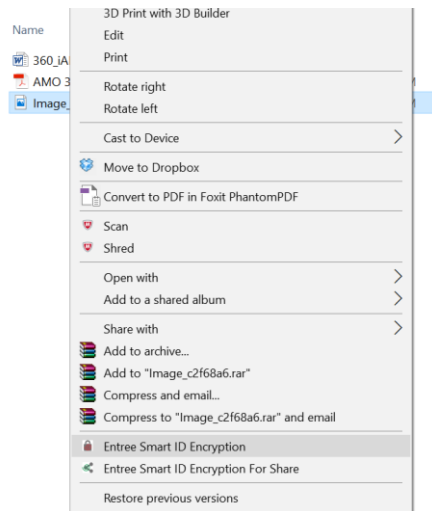


Select the private key file you backed up. Enter the password you set before.

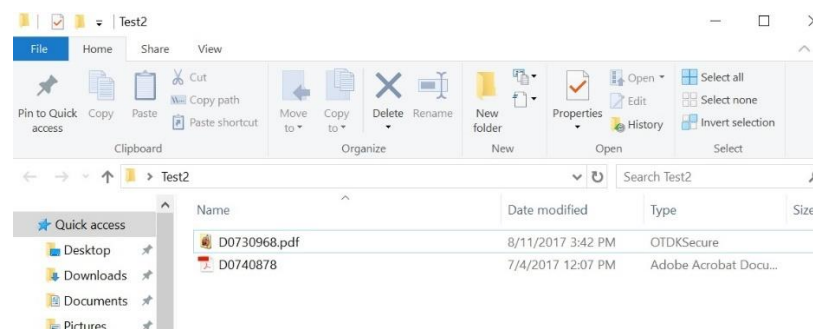


4. File/files encryption/decryption.

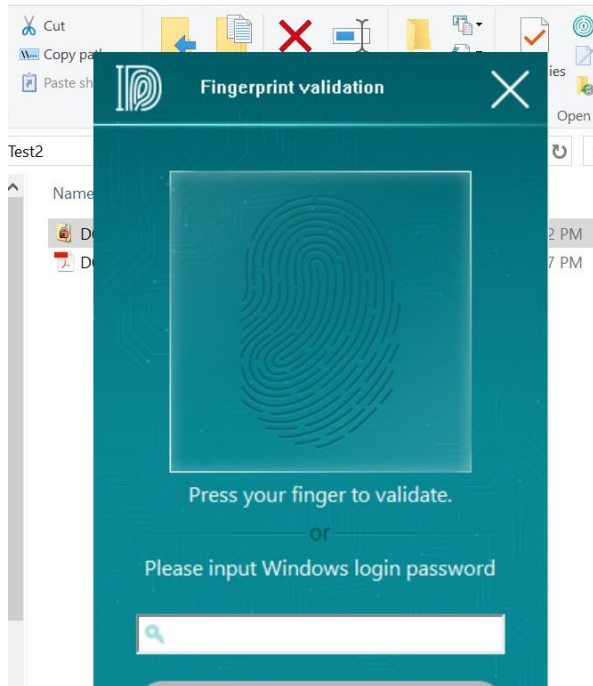
You can select file/files to encrypt. After selecting the file/files, click the right button of the mouse and select the “Smart ID Encryption” feature.



The file/files will be encrypted as the following.

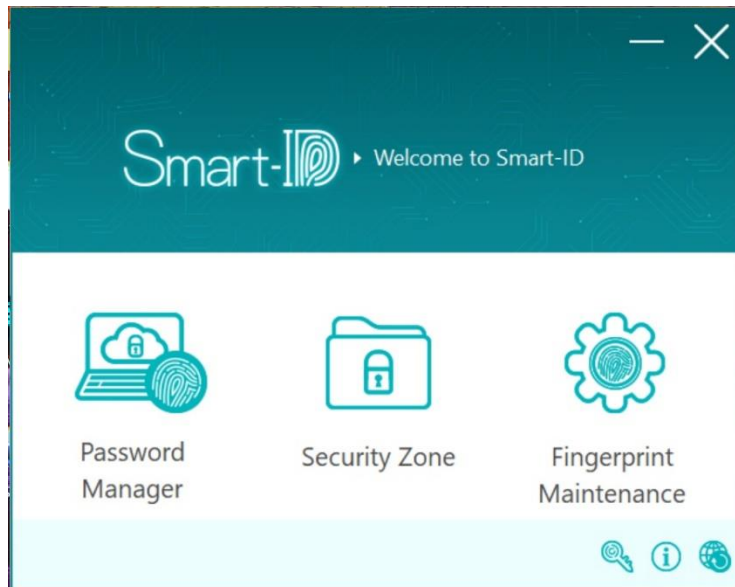


If you want decrypt the encrypted file, just double click it. The fingerprint validation window will pop up. The validation can be done by fingerprint or Windows login password.

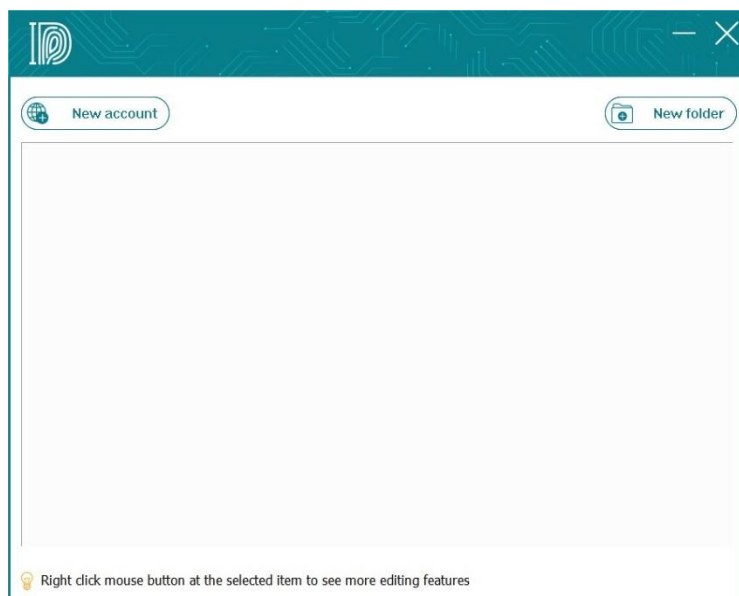


5. Password Manager

Select the “Password Manager” feature on the main panel.



The following the management panel will pop up. You can click the “New account” button to add the web site/social media account.

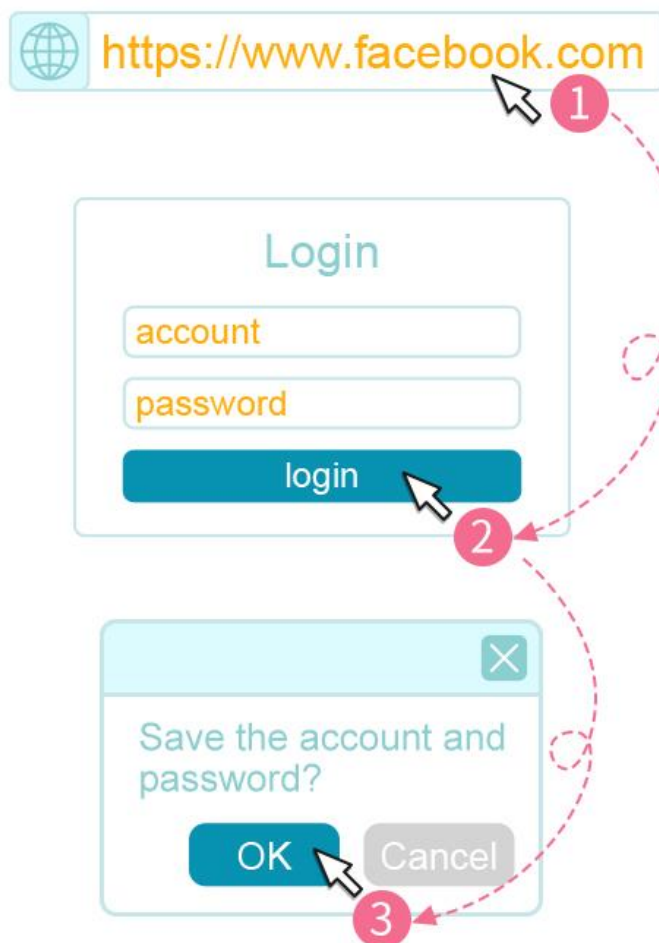


The following IE browser/Chrome will pop up. You can login the web site you would like to add. For example, Facebook. Once you finished the account and password

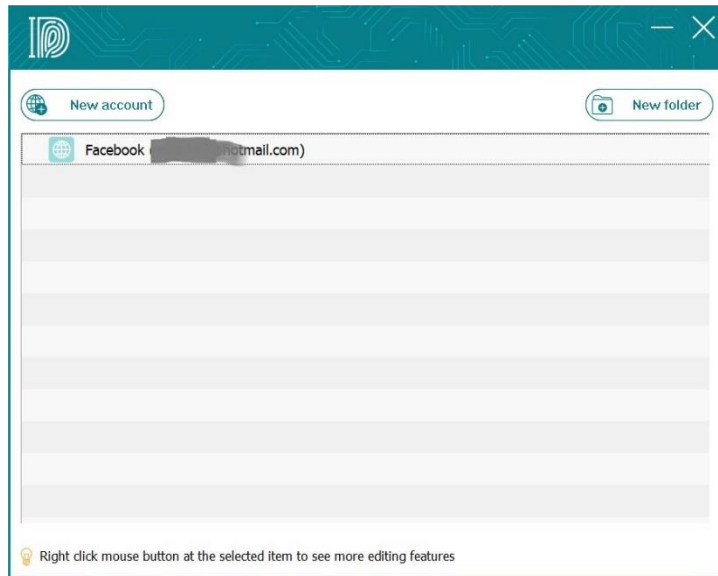
information and click “login” button, a dialog window will pop up.



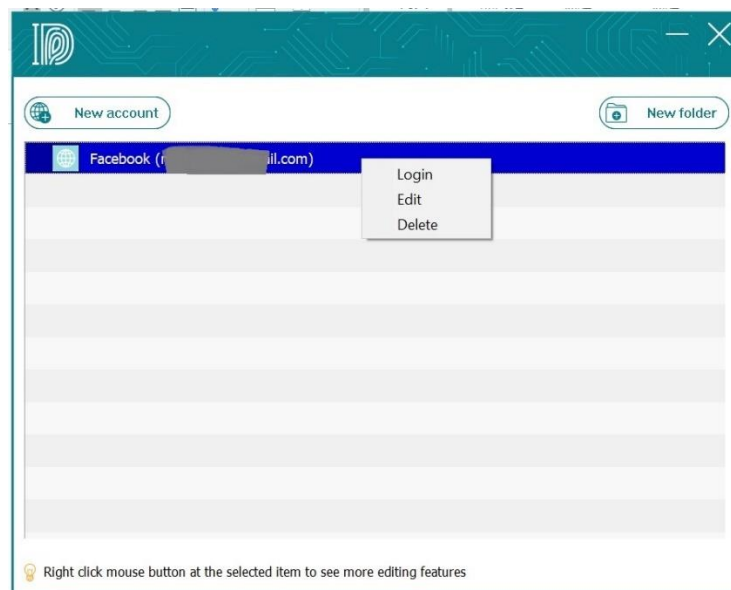
You could add more web accounts by following the below procedure.



Then, you can check the web site management window, the Facebook will be added.



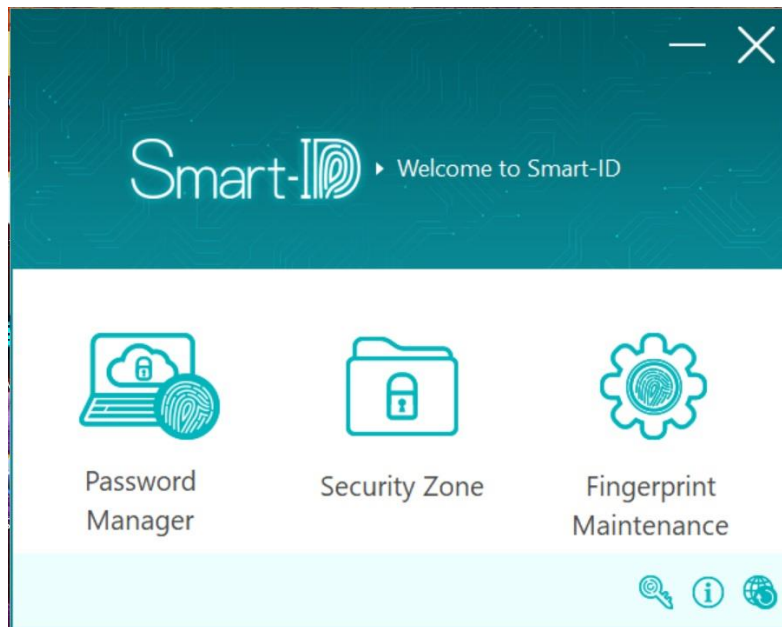
You can do “Login”, “Edit”, or “Delete” by clicking the right button of your mouse on the list.



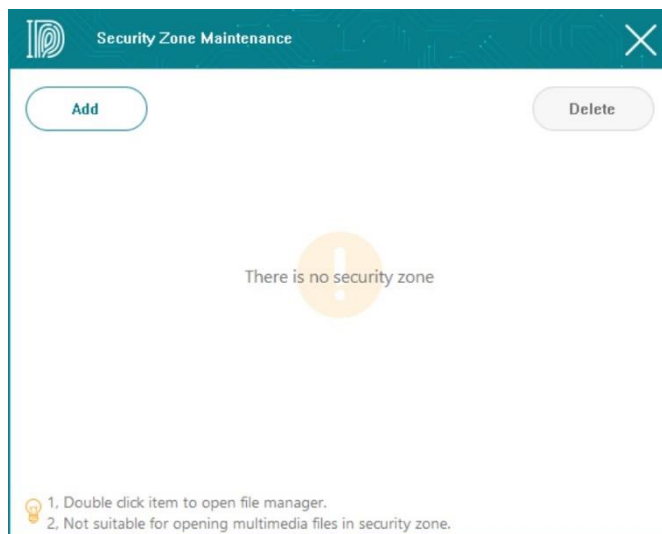
6. Security Zone

You can specify a folder as the security zone. Once a file was copied into the folder or created in the folder, it will be encrypted automatically. You could drag and drop a file/folder into the “Security Zone” icon directly. Even, you can open a file by double clicking the file. After editing and saving the file opened, it will be encrypted automatically.

Select “Security Zone” feature on the main panel.



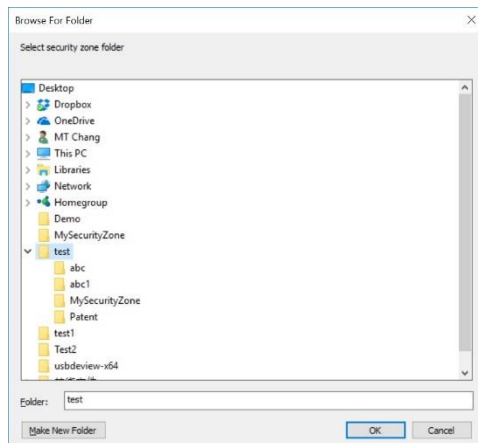
The following folder-specify window will pop up.



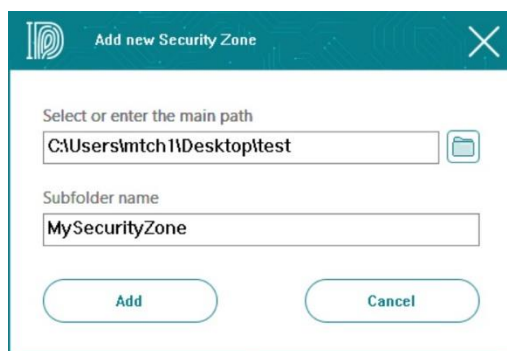
You could click the “Add” icon and the zone specify windows will pop up.



Click the rightmost button in the path specify area. The following path specify window will pop up. Then, you can select the path of the security folder.



Then, specify the Security Zone folder name in the Subfolder name.



You might leave the Subfolder name area empty.

All the files in the security folder will be encrypted automatically.

