TRIAD SECURE

HELP & GUIDE DOCUMENT

Welcome to Triad Secure, the file securing app based on the CIA Triad!

If this is your first time using the app or are confused regarding the app's functions, then you've come to the right place.

To incur regarding the app's functions, refer to the sections below:

- **Secure**
- **Backup**
- **Decryption**
- **Integrity Checker**

To incur regarding the app's forms, refer to the sections below:

- **Main Form**
- **Passphrase Form**
- **Key Configuration Form**
- **Access Control Form**
- **Integrity Checker Form**

Secure

The Secure function is done by selecting a file, choosing the hash and encryption method, inserting a passphrase, configure the key derivations, and finally configure the access control of the file.

The Secure function is done by first selecting a file.
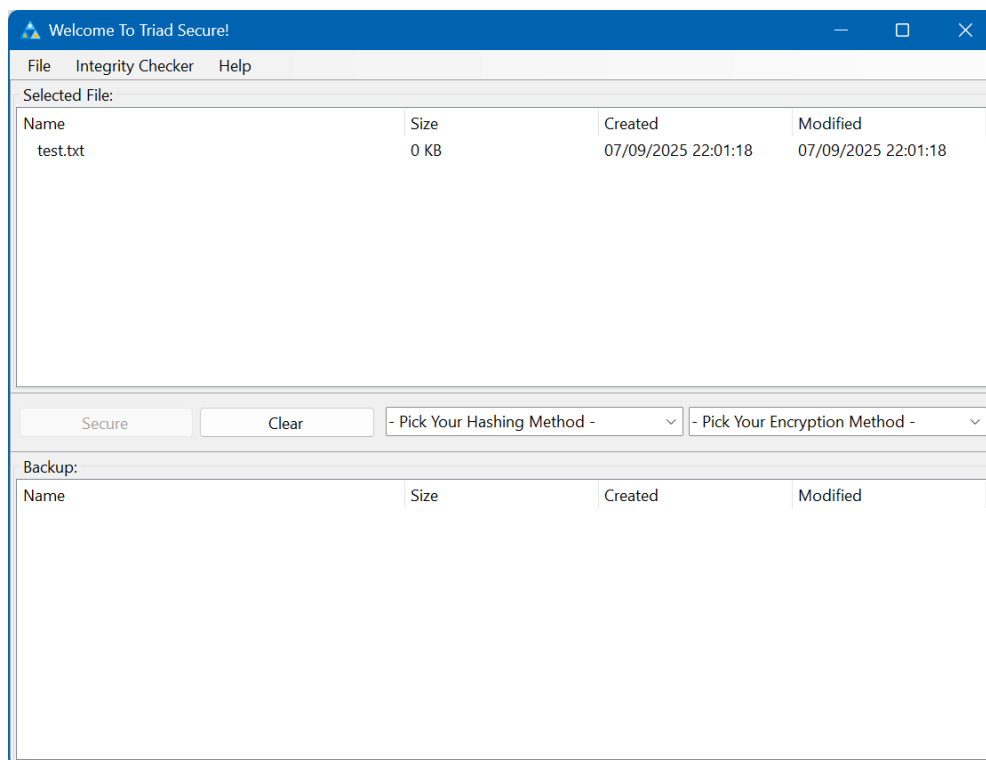
After a file has been selected, the user will select a hash and encryption method.
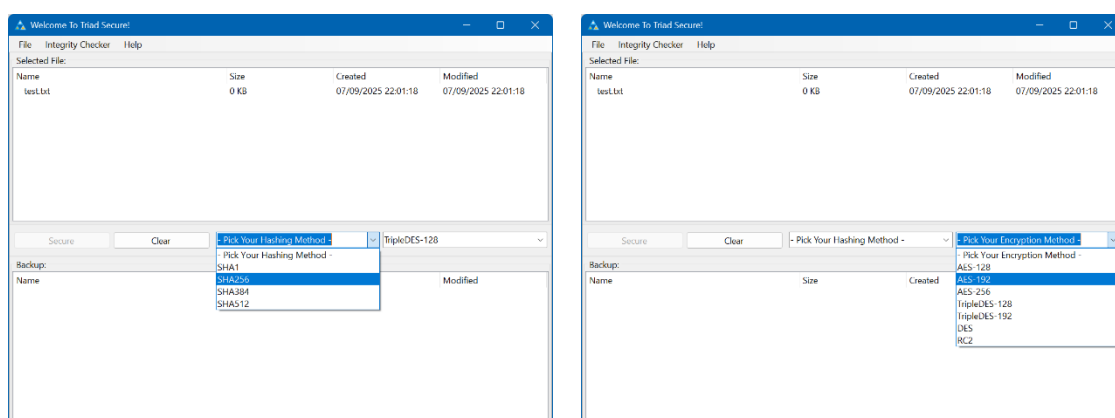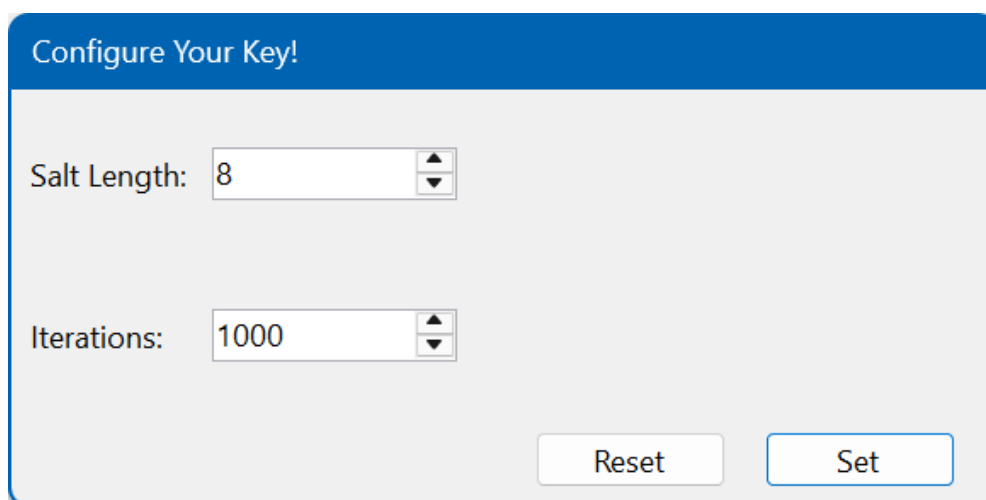

After both methods have been selected, the "Secure" button will be enabled and pressing it will start the key derivation process. The key derivation process starts with the Passphrase Form being displayed.
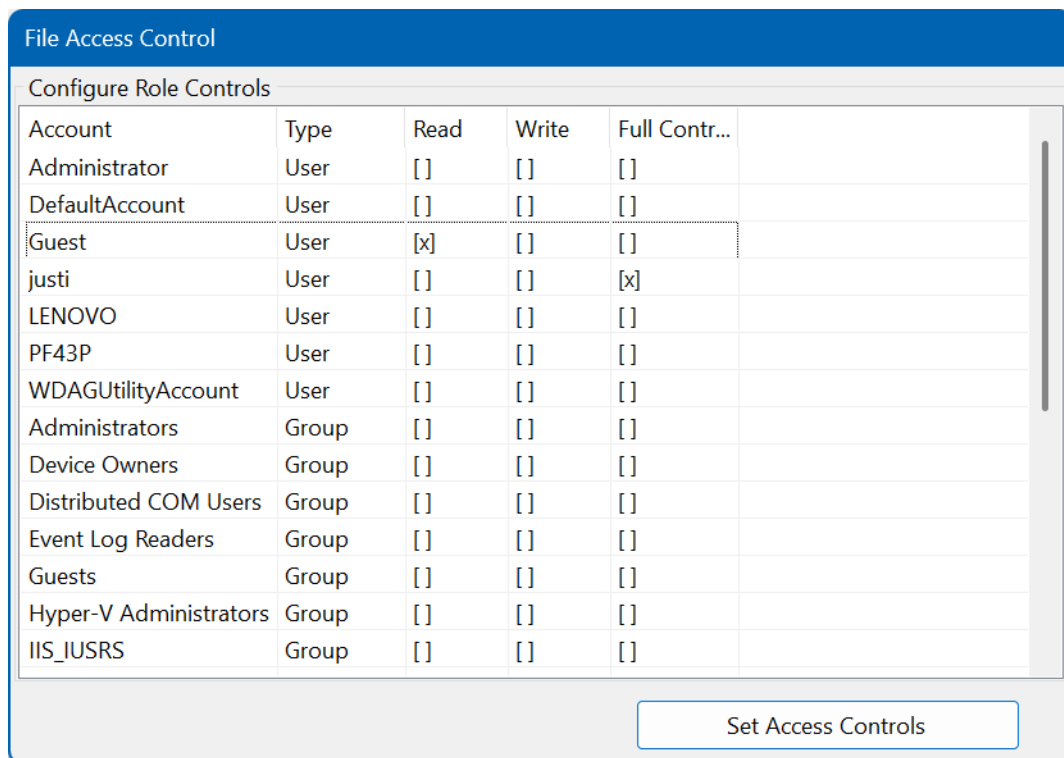
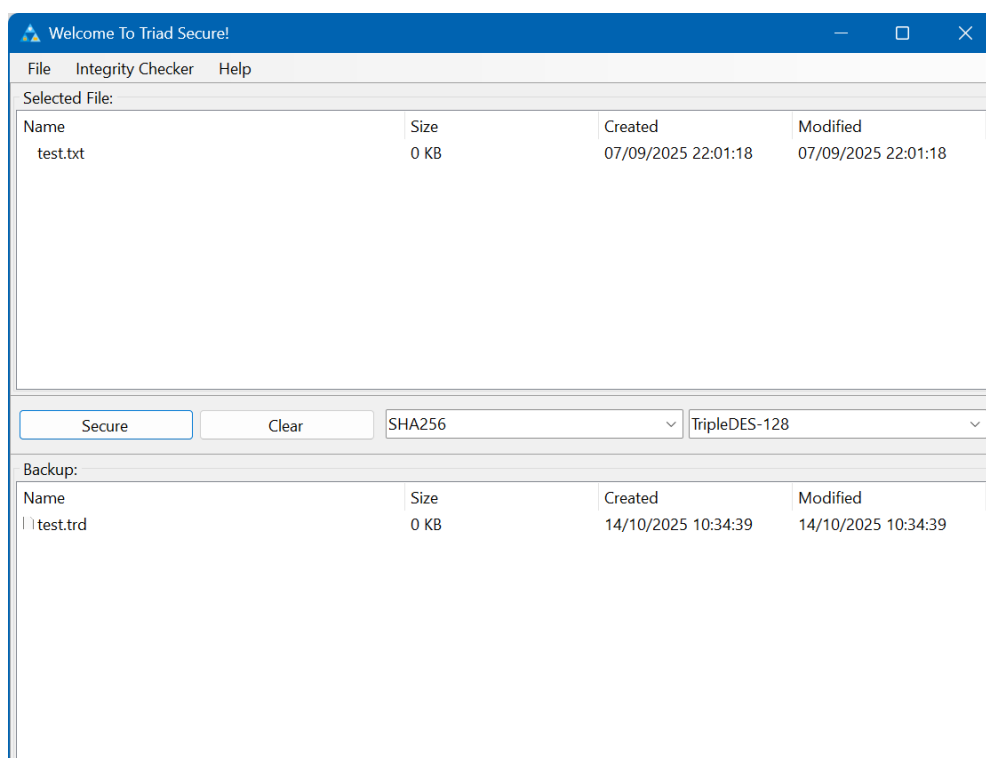The user can insert any length of passphrase they wanted as it will be hashed.
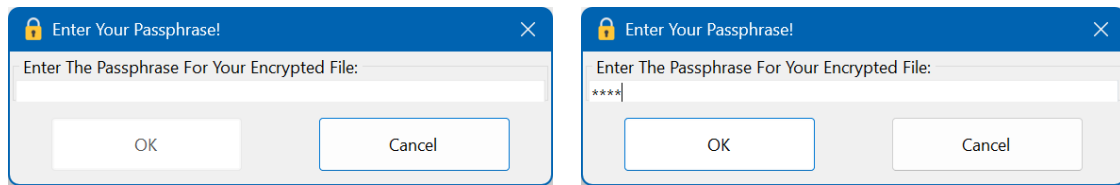
After setting the passphrase, the **Key Configuration Form** will be displayed. User will enter their desired Salt length and the number of Iterations the key derivation will run through. By default, the Salt Length is 8 (Eight) and number of Iterations is 1000 (One-Thousand). The minimum value allowed for Salt Length and number of Iterations are 8 and 1000 and the maximum value allowed for Salt Length and number of Iterations are 128 (One-Hundred-Twenty-Eight) and 10000000 (Ten-Million) respectively.

After configuring the key, the file will be encrypted with the passphrase and key configuration set before. After the file had been encrypted, the **Access Control Form** will be displayed. User will select which and what user and group can do what to the file. By default, the current user that runs the app will be selected with full control permission.

File Access Control

Configure Role Controls

Account	Type	Read	Write	Full Contr...	
Administrator	User	[ ]	[ ]	[ ]	
DefaultAccount	User	[ ]	[ ]	[ ]	
Guest	User	[x]	[ ]	[ ]	
justi	User	[ ]	[ ]	[x]	
LENOVO	User	[ ]	[ ]	[ ]	
PF43P	User	[ ]	[ ]	[ ]	
WDAGUtilityAccount	User	[ ]	[ ]	[ ]	
Administrators	Group	[ ]	[ ]	[ ]	
Device Owners	Group	[ ]	[ ]	[ ]	
Distributed COM Users	Group	[ ]	[ ]	[ ]	
Event Log Readers	Group	[ ]	[ ]	[ ]	
Guests	Group	[ ]	[ ]	[ ]	
Hyper-V Administrators	Group	[ ]	[ ]	[ ]	
IIS_IUSRS	Group	[ ]	[ ]	[ ]	

Set Access Controls

With the access control set, the file has successfully been secured, and a copy is made on the original directory and the user's **backup** folder.

Welcome To Triad Secure!

File   Integrity Checker   Help

Selected File:

Name	Size	Created	Modified
test.txt	0 KB	07/09/2025 22:01:18	07/09/2025 22:01:18

Secure   Clear   SHA256   TripleDES-128

Backup:

| Name	Size	Created	Modified
test.trd	0 KB	14/10/2025 10:34:39	14/10/2025 10:34:39

4

Backup

When the application starts, it will check if the user has their user-specific backup folder or not. If the user hadn't had their backup folder made, then the application will generate a new backup folder for the user then display all of its content in the **Backup folder List Box**. If the user already had their backup folder be generated, then its content(s) will be displayed in the **Backup folder List Box**. Anytime the user runs the **Secure** function, a copy of the file will be inserted in the backup folder and the original file directory.

Decryption

The Decryption function can be done either by using the **Decrypt** sub-menu item on a secured file (.trd extension) or by accessing the secured file copy in the backup that is displayed in the **Backup Folder List Box**.
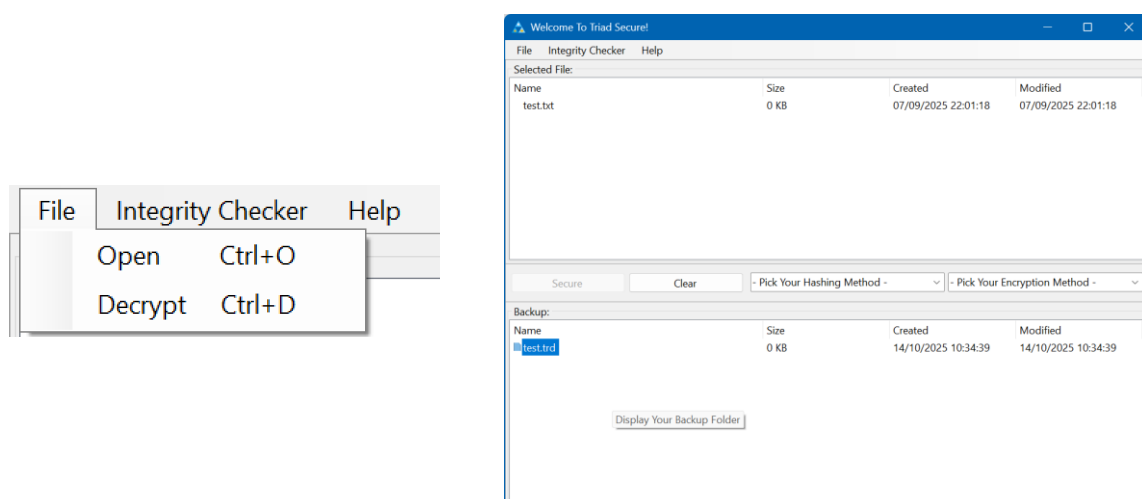
After a secured file is selected, the user will be checked if they have sufficient permission. If the user does not, it will display an error message. If the user does, the **Passphrase** form will be displayed, and the user will enter a passphrase that is related to the secured file. If the inserted passphrase is wrong, an error message will be displayed. Otherwise, the key will be rebuilt and the file decrypted then be opened with the appropriate application. On the **Integrity**

Checker function, any secured file that is selected will went through this function as well.

Integrity Checker

The Integrity Checker function is done through by first selecting the first and second file.
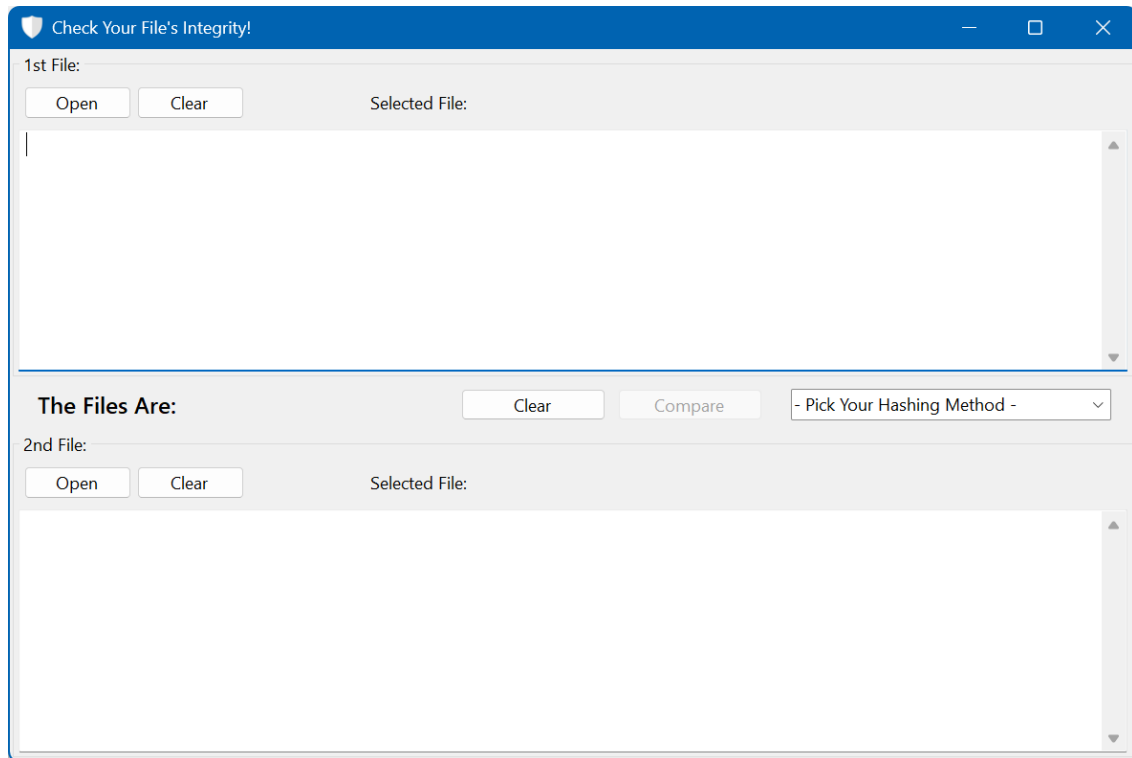
After both files has been selected, the hashing method will be chosen in which those two files will be run through to know their hash values.

After the hashing method had been chosen, the "Compare" button will be enabled and pressing the button will run the hashing algorithm on both the files. The hash values of both files will be converted into hex then be compared and displayed accordingly in the Integrity Checker Form. If a selected file is a secured file (.trd), it will go through the Decryption function

Main Form

This is the first form displayed and where the **Secure** function, the **Backup**, and the **Decryption** function reside. This form is made up of 4 sections:

– Menu Bar
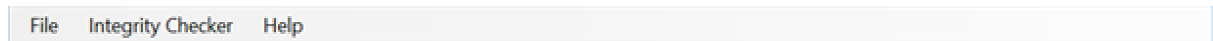
This is the main navigation and process tool. The Menu Bar is made up of several elements:

○ File, which consists of:
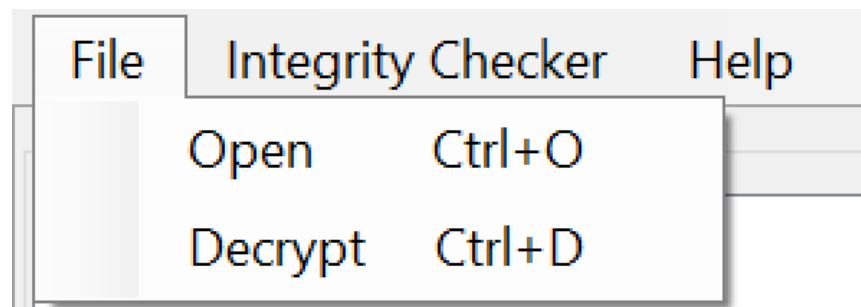
▪ Open File (Ctrl + O)

For accessing files that users want to secure. Any file that is opened will be displayed on the **Selected File List View**.

▪ Decrypt (Ctrl + D)

For decrypting and accessing secured file(s) (.trd extension). Any file that has the ".trd" extension will run through the **Decryption** process to be accessed (given that the user has the sufficient credentials and the correct passphrase).
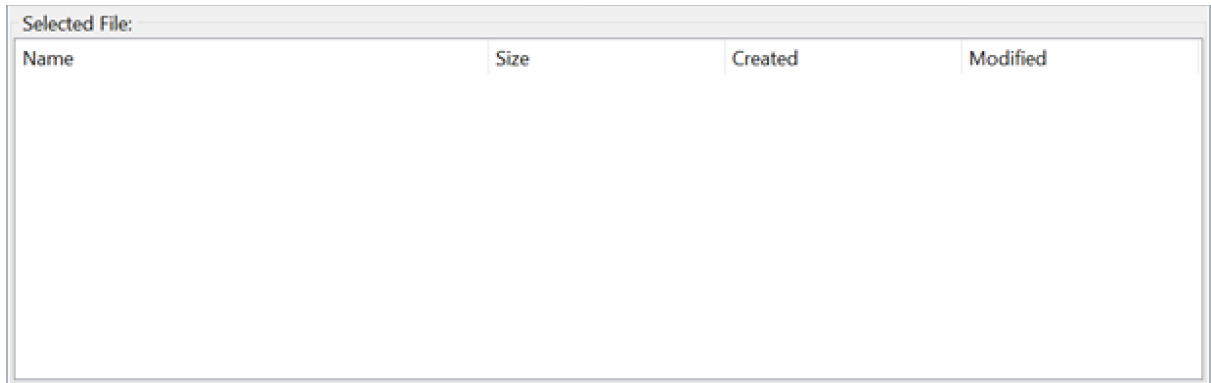
○ Integrity Checker

For accessing the **Integrity Checker Form**. The **Integrity Checker Form** contains the function to check the integrity status between two files. Information about the **Integrity Checker** function will be explained further in its own section.

○ Help

For guides and inquiries regarding the application. This is where all information and guides regarding the forms and functions of the app resides.

- Selected File List Box

Displays the currently selected file for securement. Selecting file is done through selecting **Open File** in the **Menu Bar** or by using the **Open File** shortcut (Ctrl + O). Once a file is selected, it will be displayed here.

- Main Form Control Box

Allow user to select what hash and encryption methods as well as clearing selection(s) and running the **Secure** function. The Main Form Control Box is made up of several elements:

o Secure Button

For running the **Secure** function to secure files. By default, or if there is no file selected and had not chosen the hashing and encryption methods, the button is disabled.

o Clear Button

For clearing selection(s). Any selection done (files and methods) is cleared upon button press.
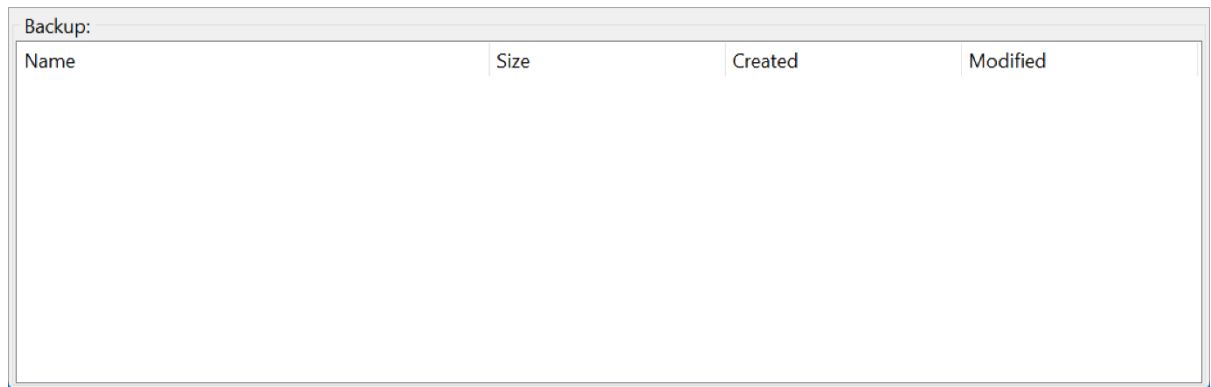
o Hash Dropdown

For selecting hash methods. List of hash methods on the **Main Form** includes: SHA1, SHA256, SHA384, and SHA512.

o Encryption Dropdown

For selecting encryption methods. List of encryption methods on the **Main Form** includes: AES-128, AES-192, AES-256, TripleDES-128, TripleDES-192, DES, and RC2.
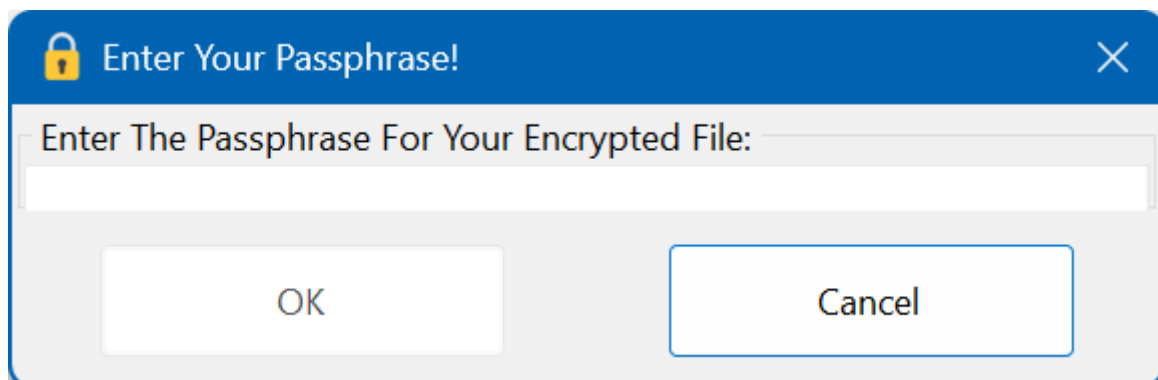
– Backup Folder List Box

For displaying Backup Folder contents. Any file that had been secured will have its **Backup** written into the Backup Folder. The Backup Folder contents can be accessed from double-clicking the item.

Passphrase Form
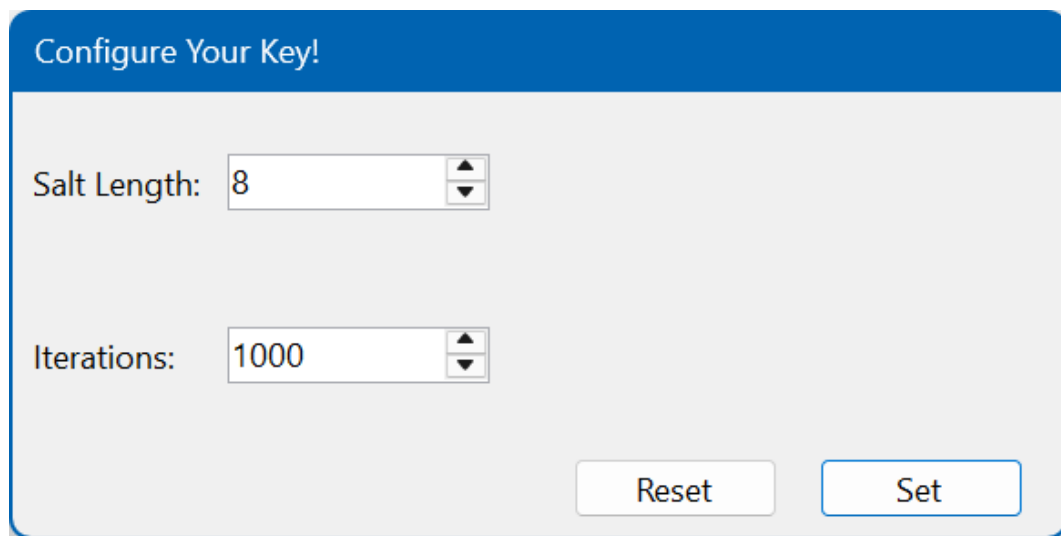
After selecting the file, hash method, key configuration as well as pressing the **Secure Button**, the Passphrase Form will be the next form displayed. User will enter any length of passphrase they wanted. The
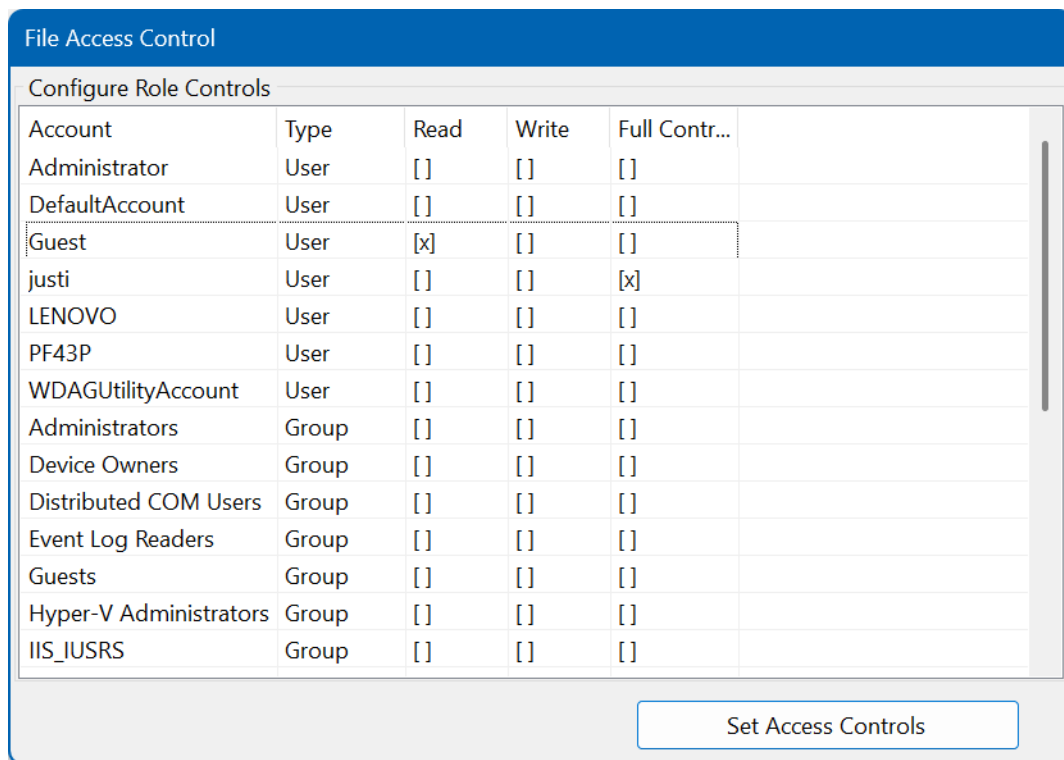
inserted passphrase will be used for making key for encryption and decryption. Pressing "Cancel" here will abort the operation. During decryption, the form will also be displayed to allow the user to enter the secured file (.trd) related passphrase.

Key Configuration Form

After inserting a passphrase, Key Configuration Form will be the next form displayed. User will enter their desired Salt length and the number of Iterations the key derivation will run through. By default, the Salt Length is 8 and number of Iterations is 1000. The minimum value allowed for Salt Length and number of Iterations are 8 and 1000 and the maximum value allowed for Salt Length and number of Iterations are 128 and 10000000 respectively.
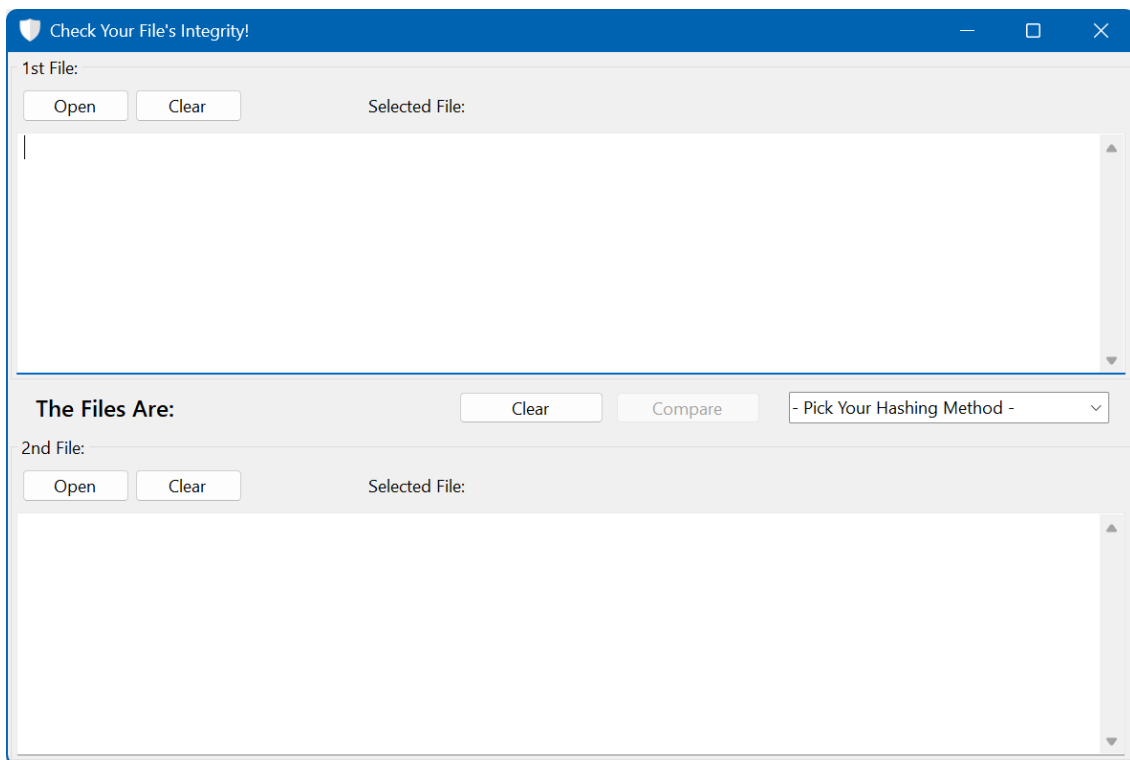
Access Control Form

Account	Type	Read	Write	Full Contr...	
File Access Control					
Configure Role Controls					
Administrator	User	[ ]	[ ]	[ ]	
DefaultAccount	User	[ ]	[ ]	[ ]	
Guest	User	[x]	[ ]	[ ]	
justi	User	[ ]	[ ]	[x]	
LENOVO	User	[ ]	[ ]	[ ]	
PF43P	User	[ ]	[ ]	[ ]	
WDAGUtilityAccount	User	[ ]	[ ]	[ ]	
Administrators	Group	[ ]	[ ]	[ ]	
Device Owners	Group	[ ]	[ ]	[ ]	
Distributed COM Users	Group	[ ]	[ ]	[ ]	
Event Log Readers	Group	[ ]	[ ]	[ ]	
Guests	Group	[ ]	[ ]	[ ]	
Hyper-V Administrators	Group	[ ]	[ ]	[ ]	
IIS_IUSRS	Group	[ ]	[ ]	[ ]	

Set Access Controls

After inserting and setting the desired Salt Length and number of Iterations, the Access Control Form will be the next form displayed. User will select which and what user and group can do what to the file. By default, the current user that runs the app will be selected with full control permission.
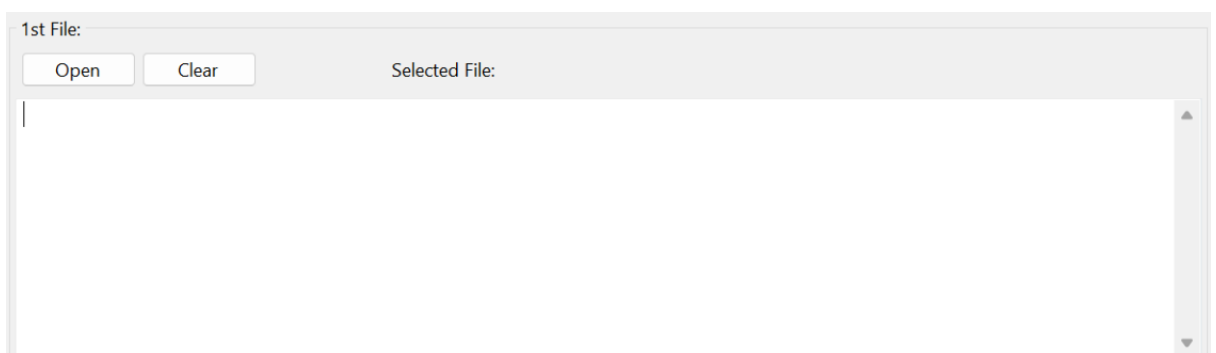
Integrity Checker Form

From clicking the <u>Integrity Checker</u> on the <u>Menu Bar</u>, The Integrity Checker Form will be displayed. The Integrity Checker Form is where the <u>Integrity Checker</u> function resides. The form is made up of 3 sections:

– First Selected File Section
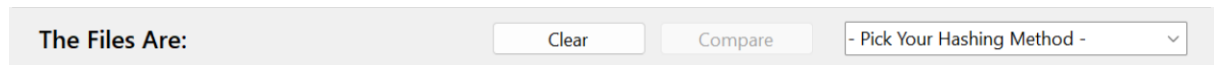
This is the First Selected File Section where operations regarding the first selected file is done for running the <u>Integrity Checker</u> function. The "Open" button is for opening a file inside the user's device. The "Clear" button is for clearing the first selected file. Any file that is opened will have its

name displayed on the right side of "Selected File:" label
(Selected File: [File Name]). Below is a textbox, which when the
Integrity Checker function is run, will display the hex of the
file's hash.

– Integrity Checker Form Control Box

The Files Are:		Clear	Compare	- Pick Your Hashing Method -

Allow user to select what hash method as well as clearing
selection(s) and running the Integrity Checker function. The
Integrity Checker Control Box is made up of several elements:

o Comparison Label

For displaying the status of comparison between the first
and second selected file. Status will be displayed on the
right side of the label and will display either "A Match"
or "Not A Match" (The Files Are: [A Match/Not A Match]).

o Clear Button

For clearing selection(s). Any selection done (files and
methods) is cleared upon button press.

o Compare Button

For running the Integrity Checker function to compare the
integrity status between the first and second selected
files. By default, or if there is no file selected and had
not chosen the hashing method, the button is disabled.

o Hash Dropdown

For selecting hash methods. List of hash methods on the
Integrity Checker Form includes: MD5, SHA1, SHA256, SHA384,
and SHA512.

– Second Selected File Section
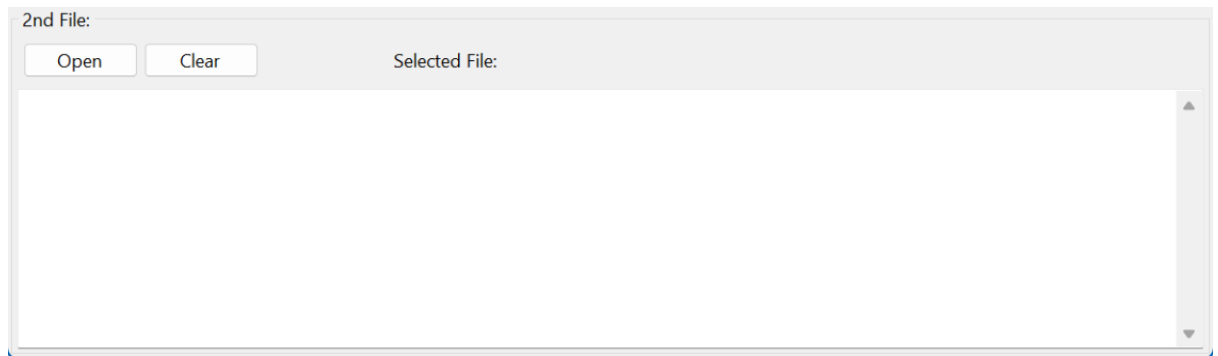
This is the Second Selected File Section where operations regarding the second selected file is done for running the **Integrity Checker** function. The "Open" button is for opening a file inside the user's device. By default, the folder first opened when using the "Open" button will be the **Backup** folder. The "Clear" button is for clearing the second selected file. Any file that is opened will have its name displayed on the right side of "Selected File:" label (Selected File: [File Name]). Below is a textbox, which when the **Integrity Checker** function is run, will display the hex of the file's hash.