TRS File Monitor

User Guide

翊捷資訊股份有限公司

Team Rise System Co., Ltd.

4F, 8-1 Han Chou S. Road, Sec. 1, Taipei, Taiwan, R. O. C.

TEL:886-2-23221622 FAX:886-2-23223986

Invoice No:96943675

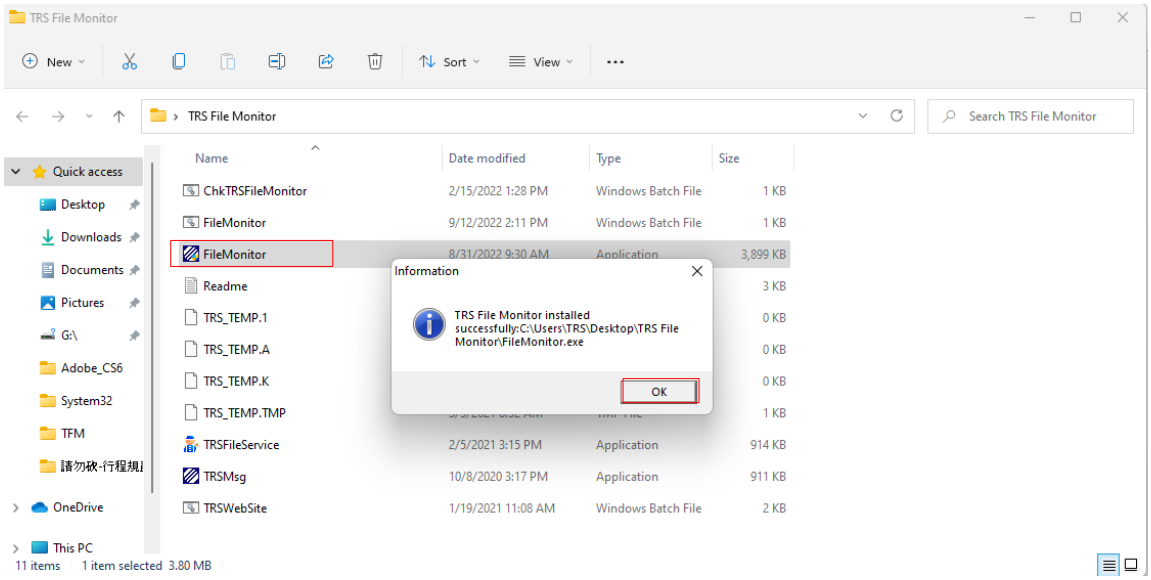
DATE：2022/09/12

Contents

1. Start TRS File Monitor

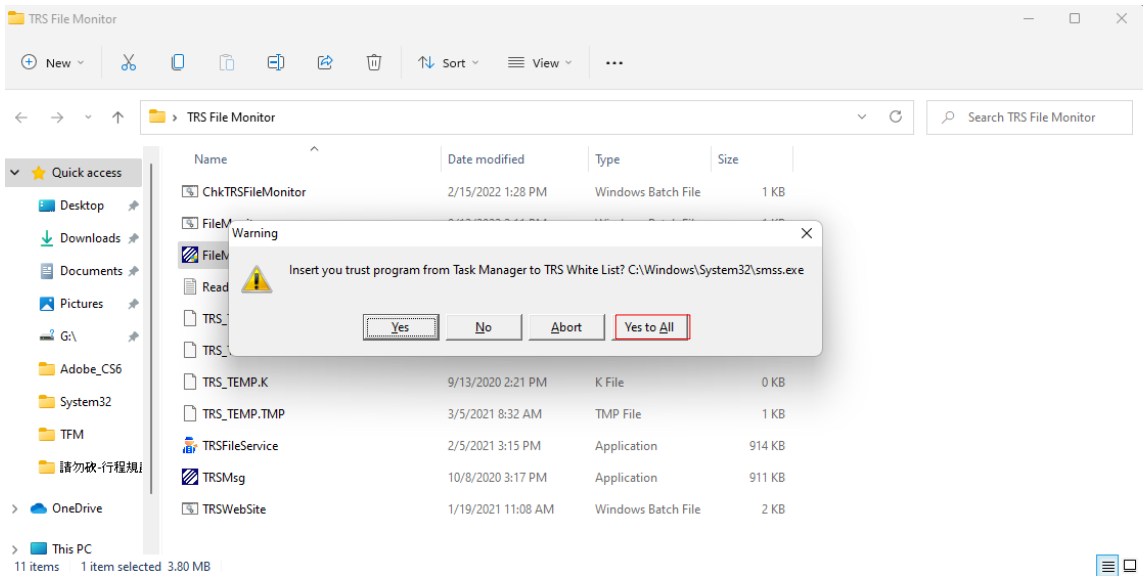
1.1 TRS File Monitor installation

Double-click the program and the User Account Control window will appear. Click Yes to install it smoothly. After the installation is successful, click OK to start TRS File Monitor.



1.2 Automatically add to the White List

After the installation is successful, whether to add the currently open program to the whitelist will appear when using it for the first time, according to the work administrator



Button-Yes : Add to the White List one by one according to the files in the message window.

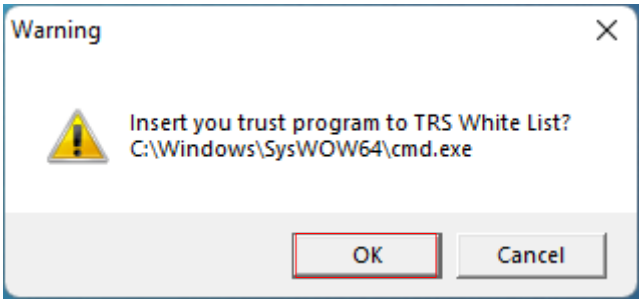
Button-No : According to the files in the message window, do not add to the White List one by one.

Button-Abort : Skip all.

Button-Yes to All: add all (recommended selection).

1.3 Warning

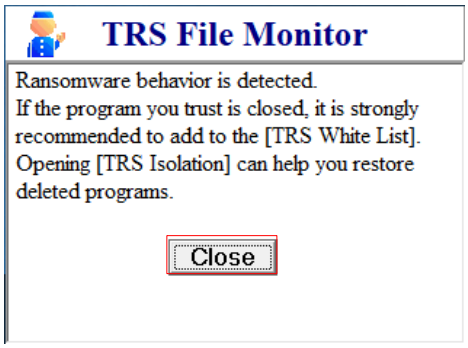
If [Yes to All] is not selected in item 1.2, the following message may appear.



1.4 Popup window

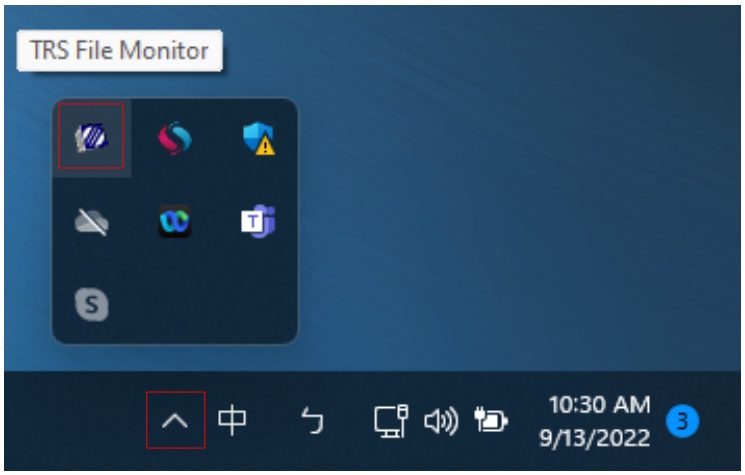
If [Yes to All] is not selected in item 1.2, the following message may also appear.

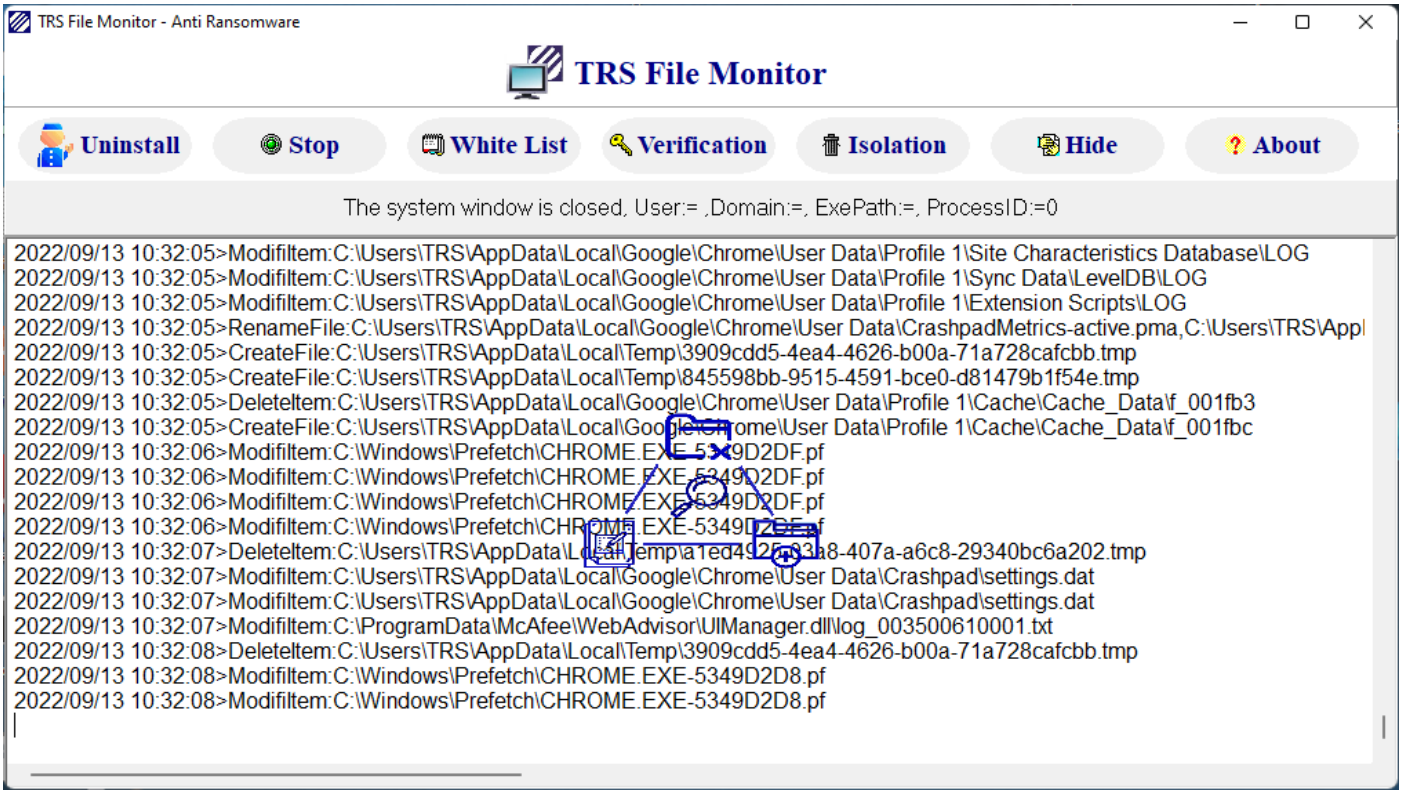
TRS File Monitor detects suspicious behavior, a window will appear at the bottom right of the screen and the program will be moved to quarantine.



1.5 TRS File Monitor operation

RS File Monitor runs in the background and does not affect user operations. You can click the icon in the toolbar to see the real-time detection screen and use other button functions.

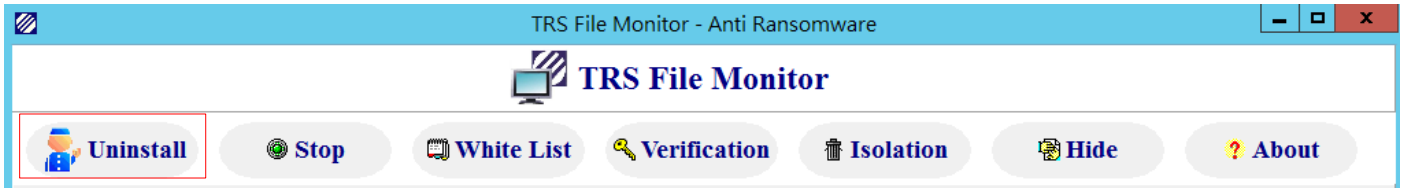




2. TRS File Monitor button function

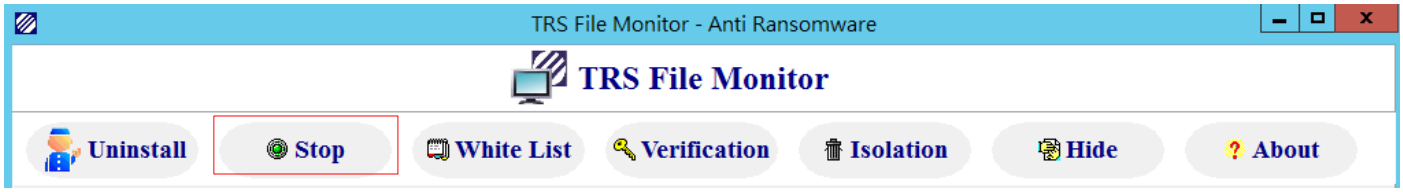
2.1 Uninstall

After clicking the button, the program will be uninstalled.

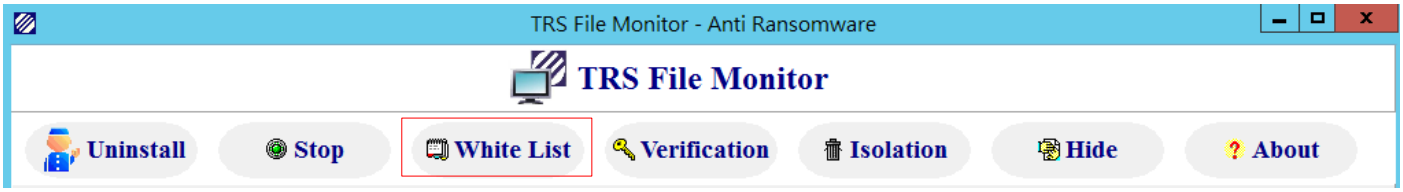


2.2 Stop

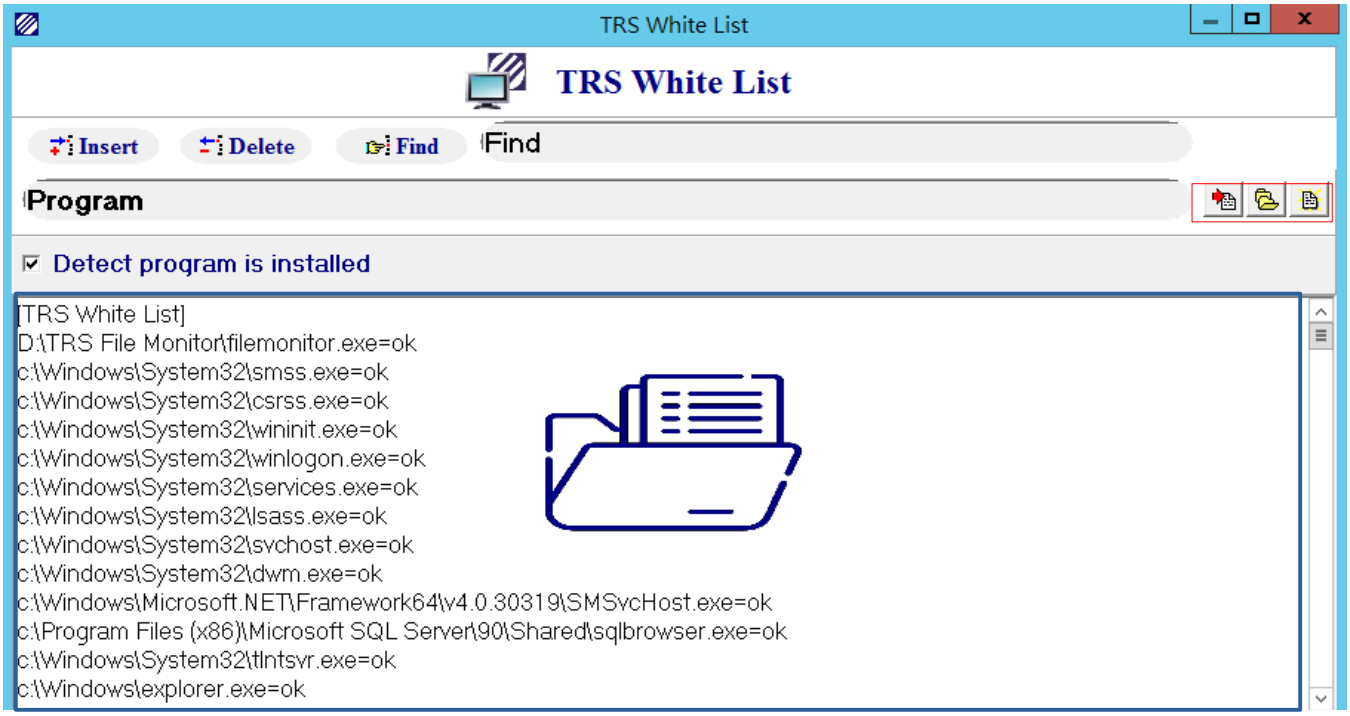
When the button is clicked, the detection stops.



2.3 White List



There are three ways (in the red box) to add trusted programs to the White List to avoid misjudgment by TRS File Monitor, and the blue box below is the programs currently in the White List.



2.3.1 Adding Frequently Used Programs from administrator

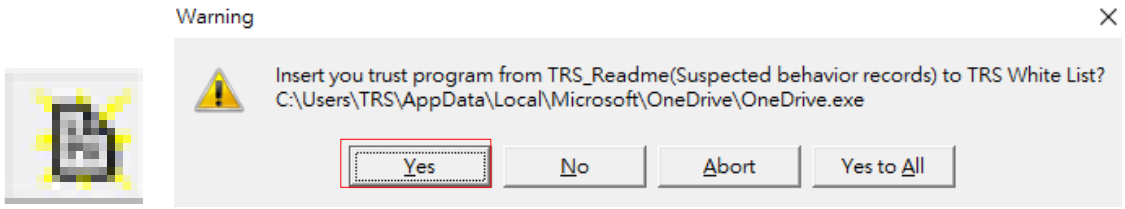
TRS File Monitor will detect frequently used programs from administrator and add them directly to the White List.

2.3.2 The user adds the program from the file path

Users can select trusted programs to be added to the White List by file path

2.3.3 Add to the White List from sequences detected as suspicious programs

TRS File Monitor will record suspicious programs in TRS_Readme.txt. Users can click this button to add trusted programs detected as suspicious programs. This button will display the message of whether to add to the White List one by one



Yes : Add to the White List one by one according to the files in the message window

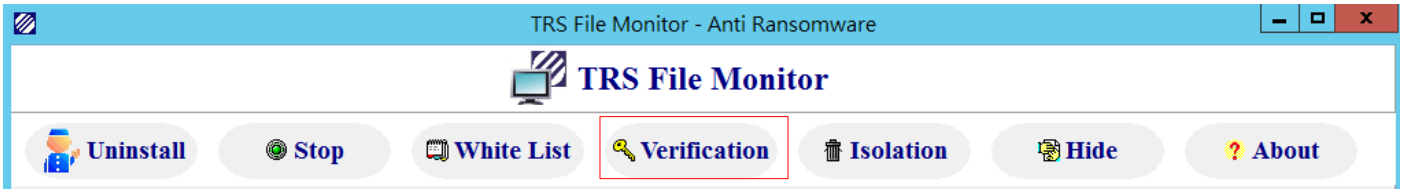
No : According to the file in the message window, do not add to the white list one by one。

Abort : Skip all.

Yes to All : add all (not recommended).

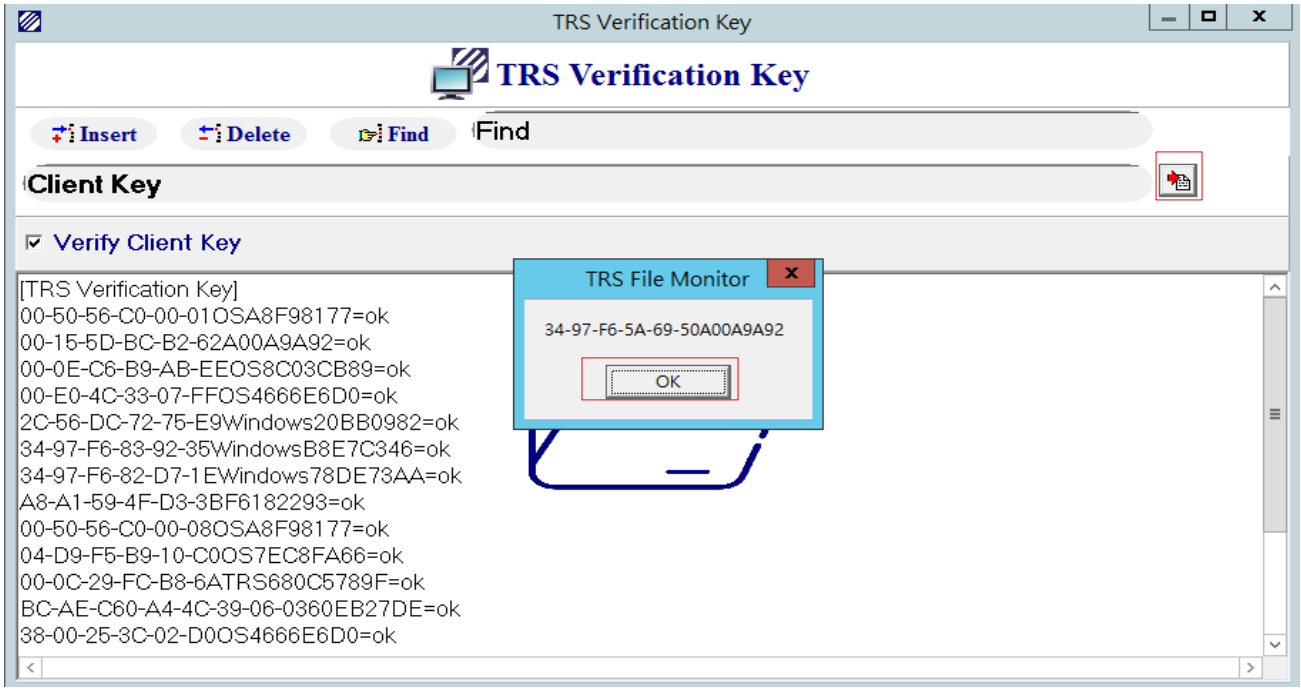
2.4 Verification

TRS File Monitor provides authentication for RDP login in a multi-person environment, and can use the hardware authentication function to add a layer of protection.



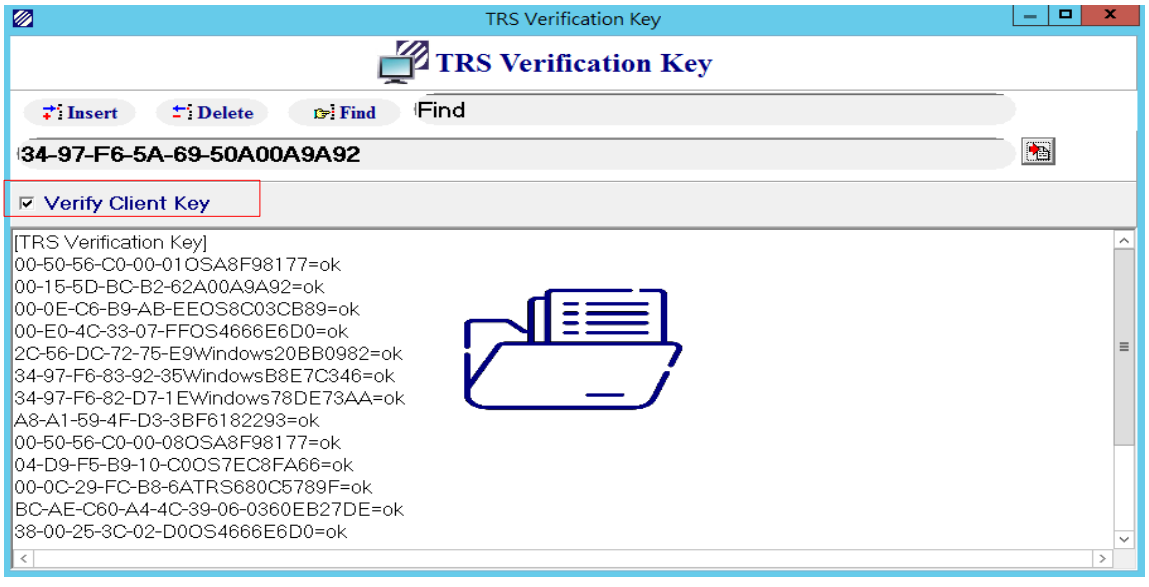
2.4.1 Checking the machine code

After clicking the button, the local machine code can be displayed and copied to the system administrator for adding to the remote host.



2.4.2 Enable hardware verification

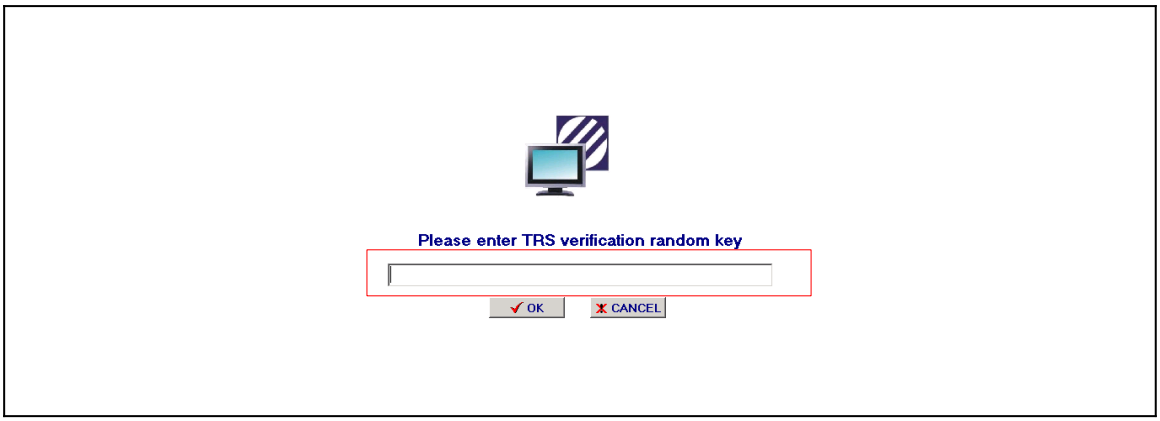
Turn on the hardware verification function (red box) on the TRS File Monitor of the remote host. As long as the host of the user to be connected has been added to the list, you can



connect to the remote host without entering the verification code.

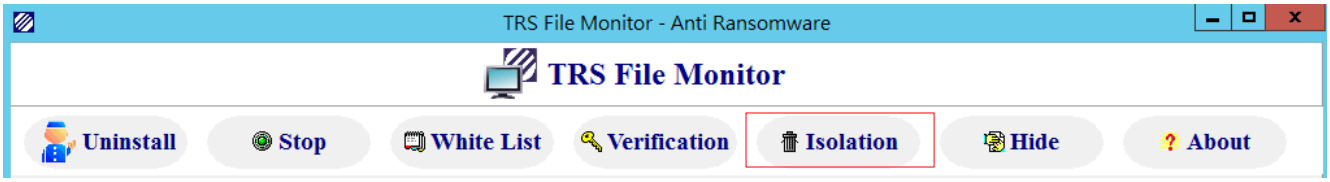
2.4.3 Random number verification code

If the user does not have TRS File Monitor installed, in order to connect to the remote host, in addition to entering the user's password for the original RDP connection, the user must also enter the password according to the customized random number, in order to successfully enter the remote host.



2.5 Isolation

When an application behaves like ransomware, it may be moved to the quarantine area to protect the user's operating environment.

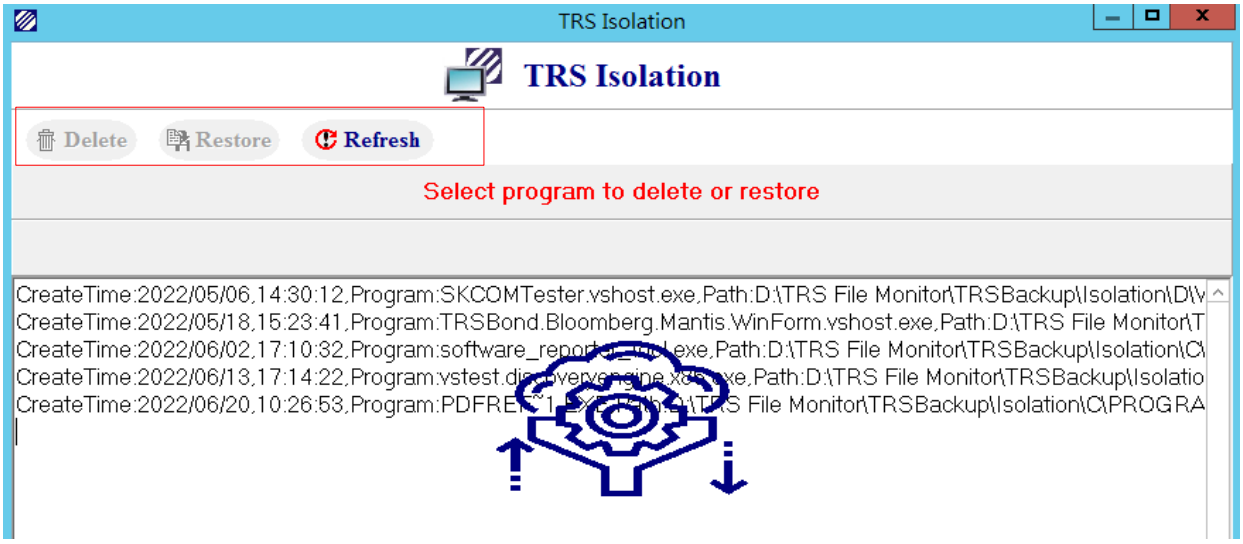


2.5.1 Restore

If a trusted program is added to the quarantine area and cannot run smoothly, it can be restored in the quarantine area, the program will be automatically added to the White List, and the program will be restored to the original installation path.

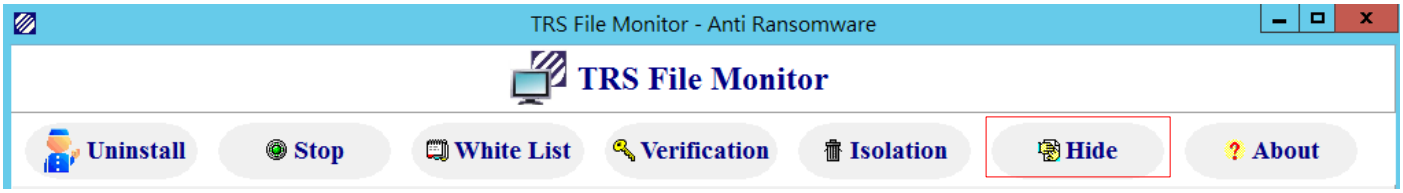
2.5.2 Delete

If a suspicious program appears in the quarantine area, the program can be deleted directly through TRS File Monitor.



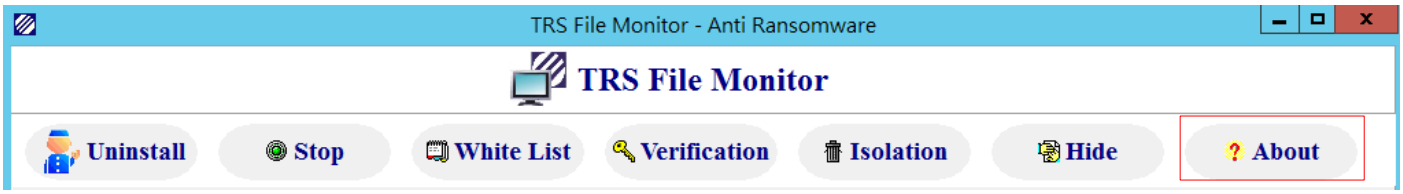
2.6 Hide

If users want to hide TRS File Monitor on the desktop, they can click Hide to return the program to the background operation. This action does not affect the detection.



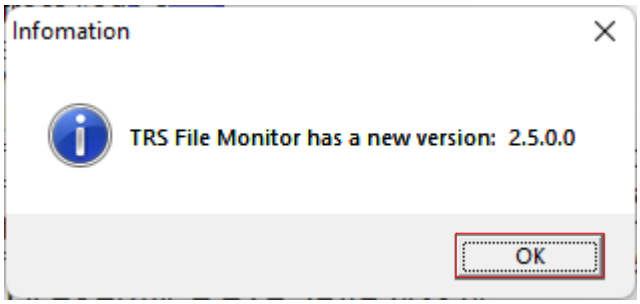
2.7 About

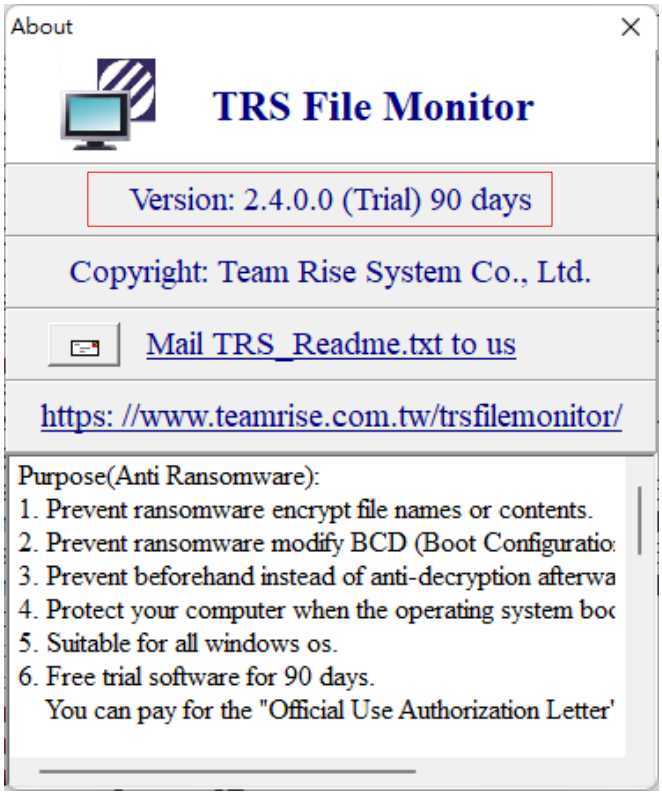
The version information of TRS File Monitor is located on this tab, which can provide users with confirmation whether the current version is the latest version.



2.7.1 Release information

If the version of the user's computer is not the latest version, a prompt window will pop up, and the red box is the remaining days of the trial.



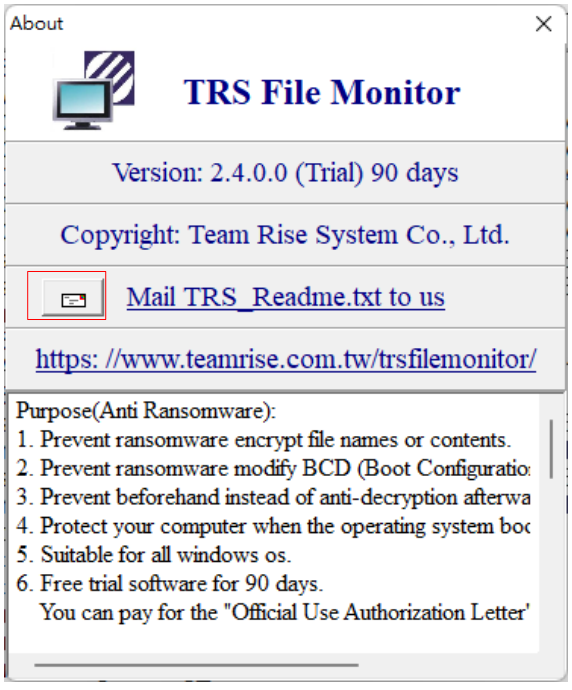


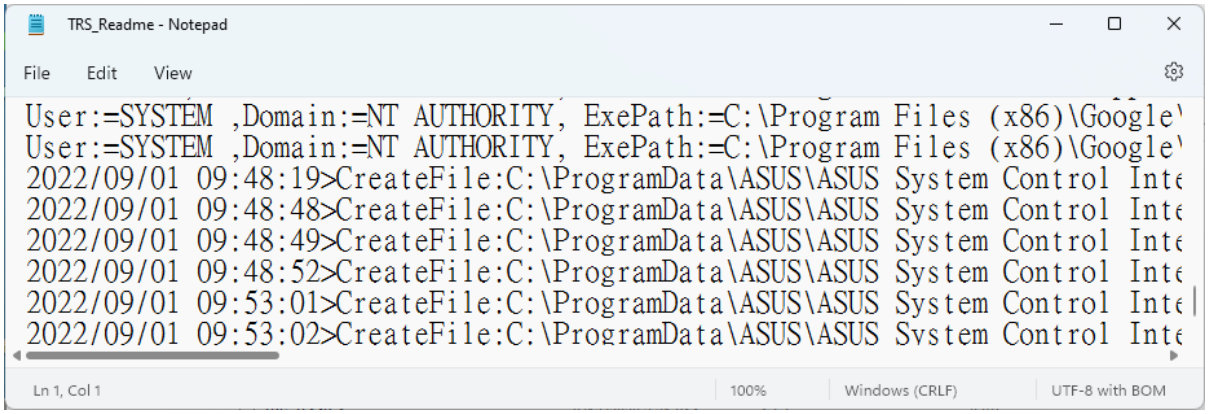
2.7.2 Contact the TRS File Monitor team

You can click the website to enter the official website to learn more about this product and contact us.

2.7.3 Detection report

TRS File Monitor will record the time and the list of files suspected of ransomware. This button can generate a list for follow-up.

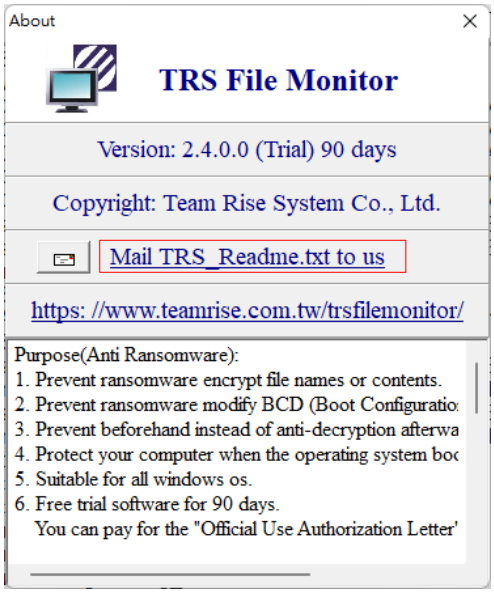


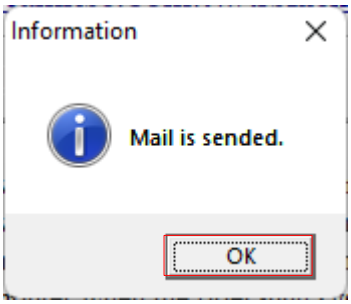


2.7.4 Send report to TRS File Monitor development team

If you have any doubts about the detection report, you can send the report in this way for the development team to contact you further.

※There is no risk of personal information leakage in this content





3. Frequently asked questions

3.1 Why Install TRS File Monitor?

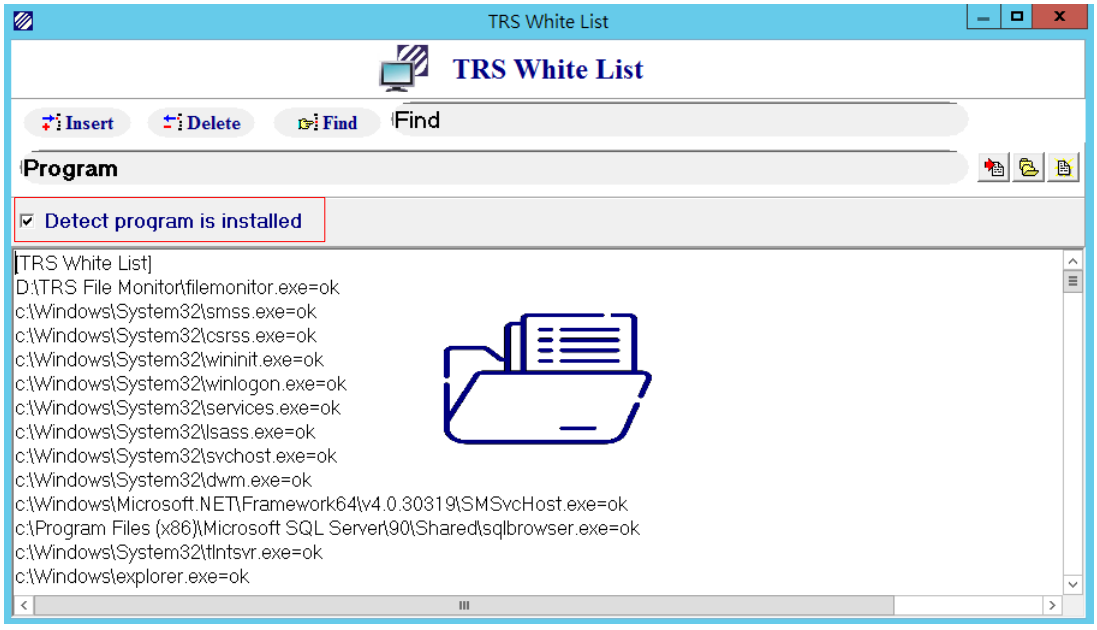
- With a concept and method different from other anti-virus or anti-ransomware, it can block Ransomware that the world-renowned anti-virus or anti-ransomware cannot block.
- When suspicious Ransomware behaviors are detected, the files are prevented from being changed in time or even beforehand.
- From a common behavior of creating, renaming or deleting files, it can be determined whether it is suspicious Ransomware.
- Prevent Ransomware from modifying BCD (boot configuration database).
- An additional layer of protection against RDP (Remote Desktop Connection).

3.2 Differences between the free trial version and the paid version of TRS File Monitor. .

Features	Free	Premium
Detect and prevent extortion	✓	✓
Personal service	×	✓
Customized service	×	✓ (such as 3.21)
Authorization	×	✓
Use period	90 days	Annual fee
Regardless of the free trial or the paid version, information security is not absolutely secure, and it requires user feedback to keep the functions up to date		

3.3 When installing a new program, it was blocked by TRS File Monitor, which made the installation impossible.

- Check [Detect Program is installed] on the White List tab, you do not need to end the program, but after installing the program for security, remember to check back to [Detect Program is installed]



- You can directly click the Stop button (such as 2.2) to stop the detection. After the installation is successful, click Start again to resume the detection.

3.4 TRS File Monitor was tested to block the following ransomware :

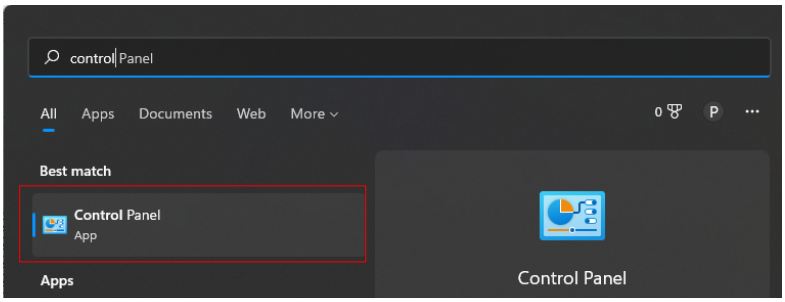
Reveton、CryptoLocker、TorrentLocker、CryptoWall、KeRanger、RSA4096、Mischa、WannaCrypt、Petya、Bad Rabbit, Helps users to perform normally in a safe environment.

3.5 Computer specifications for installing TRS File Monitor.

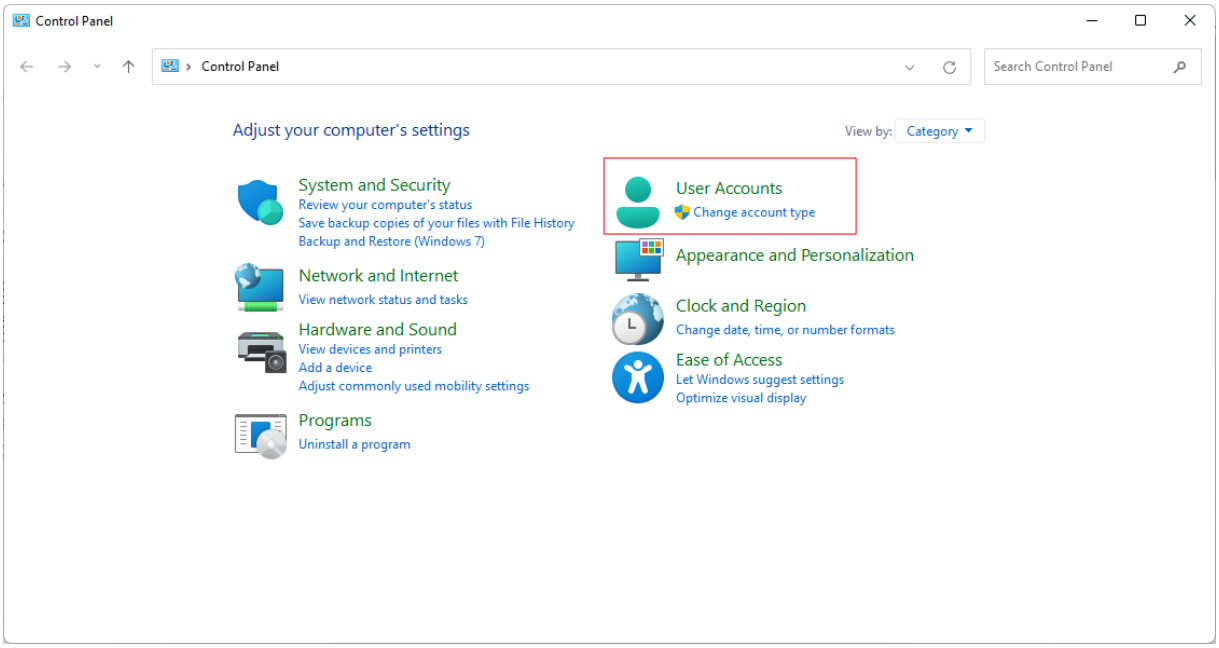
- Microsoft Windows Server 2008 Standard or above (including x86, x64)
- Microsoft Windows 7 Home Premium and above (including x86, x64)
- It is strongly recommended to enable UAC (User Account Control), as detailed in Section 3.6

3.6 UAC (User Account Control) is strongly recommended.

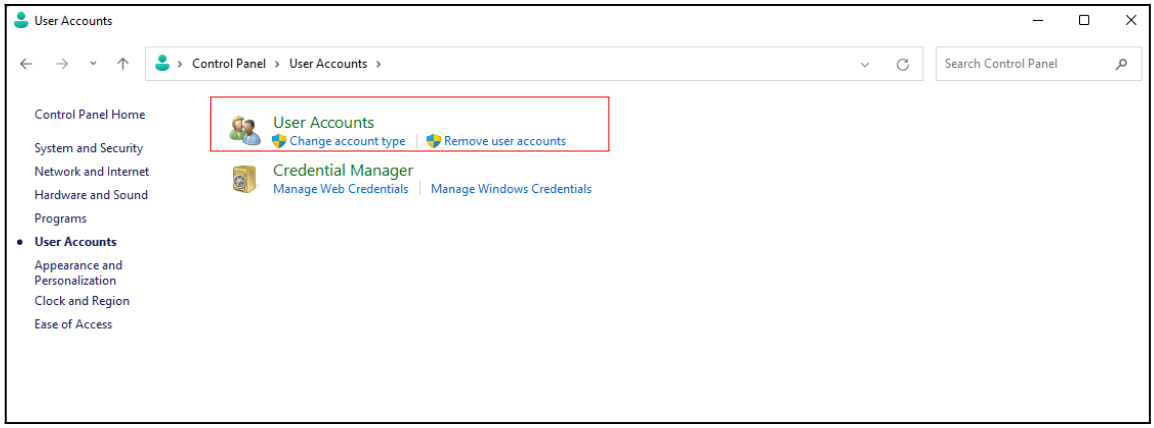
Step1 : Type in the computer search tool - console panel



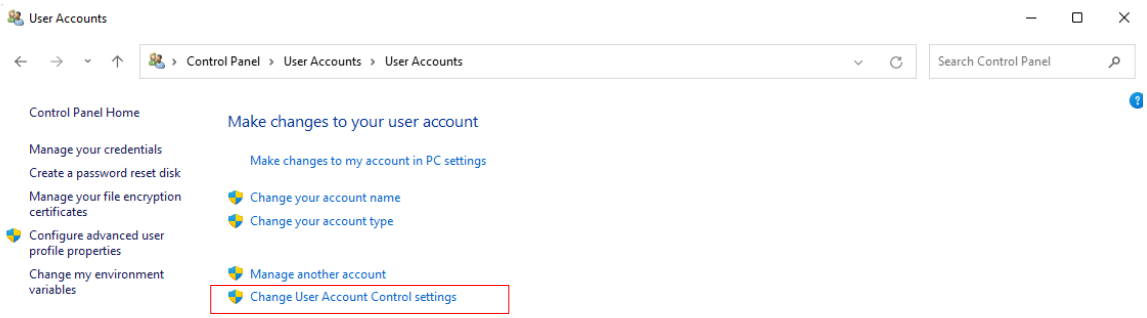
Step2 : Click on [User Accounts]



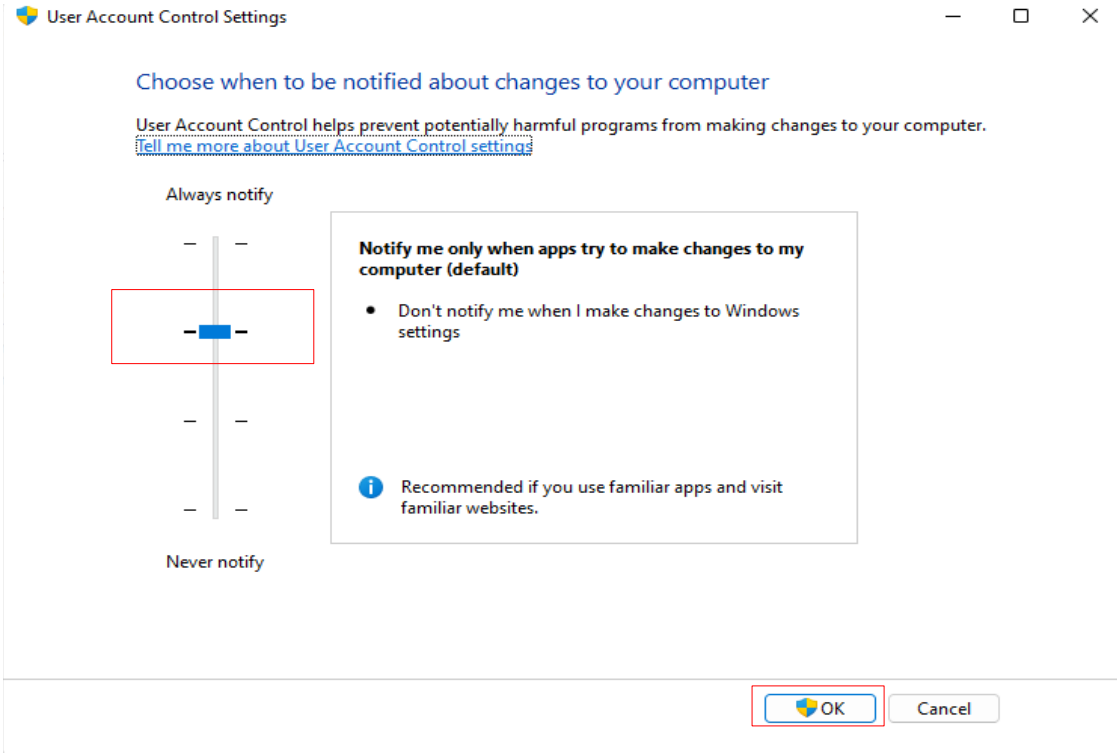
Step3 : Select[User Accounts]again



Step4 : Enable UAC (Using Account Control), select "Change User Account Control Settings"



Step 5 : Pull the left side back to the initial value as shown in the red box, and then select [OK]



Step 6 : You need to restart the computer for the setting to take effect.

3.7 Why am I still being asked to enter the machine code even though hardware verification is turned on?

- You can first check whether the machine code has been added to the Server's TRS File Monitor verification list
- Make sure that TRS File Monitor is installed.
- Check whether TRS File Monitor stops detecting. For details, see Section 2.2.
- The clipboard function of Windows Remote Desktop Connection must be checked to perform client hardware authentication. For details, please refer to chapter 3.14

3.8 Sever has installed TRS File Monitor, but it is not installed on this machine. Why does it log out and jump back to this machine when entering random numbers?

- In order to prevent hacker attacks, TRS File Monitor locks the keys that are not related to the machine code. Once the user touches it, it will open the protection mode and log out directly from the server.
- The user can only use: "Ctrl", English, number, "-" and other keys, otherwise it is regarded as a hacking attack.
- Press ALT and other keys to try to leave the verification screen.
- In order to prevent hackers from using various methods to guess the random code, the system is set to complete the input within 30 seconds, and log out if the input is not completed after 30 seconds

3.9 Can't see the TRS File Monitor Icon in the Windows taskbar?

- Insufficient user permissions, security considerations, system administrators can see and use
- Because the protection is activated without logging in after booting, sometimes in the console mode, the system administrator can log out and then cancel the logout, and then the system can see the information.

3.10 Press Stop of TRS File Monitor to stop monitoring, will it also stop the ransomware prevention function?

In single-player mode: But in a multi-session environment (Multi Session), the anti-ransomware function is still preserved.

3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end?

When you press the end or are forced to end, it will be automatically restarted, unless you manually uninstall (Uninstall)

3.12 Does the ransomware prevention feature also stop when the system is logged out?

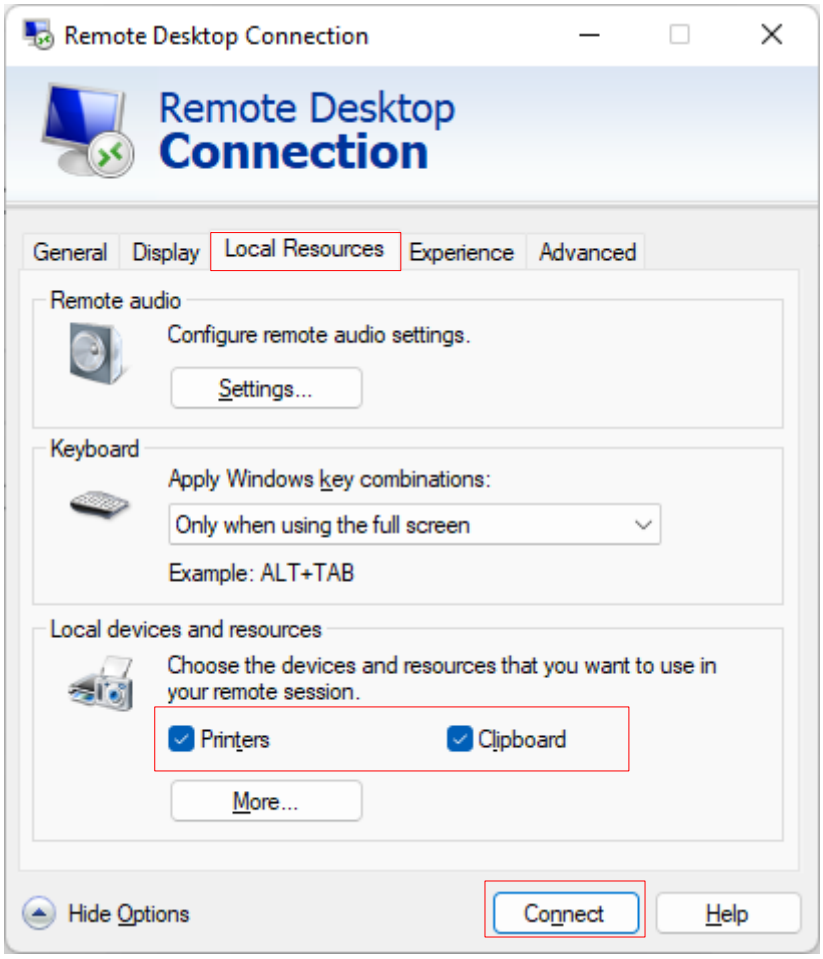
When the system is logged out, the anti-ransomware function is still maintained; in the console mode, a warning message will appear when the system is logged out, and the anti-ransomware function will not be affected.

3.13 How do I know if a suspicious ransomware behavior is detected?

- The following warning message screen will appear in the login state, as detailed in chapter 1.4
- Enter the quarantine area to see the quarantined programs sorted by date. If the program is repeatedly quarantined, only the first date will be displayed. For details, see Chapter 2.5
- Click the About mail icon to view the suspected ransomware behavior and quarantine records, as detailed in Section 2.7.3.

3.14 What is the verification function for?

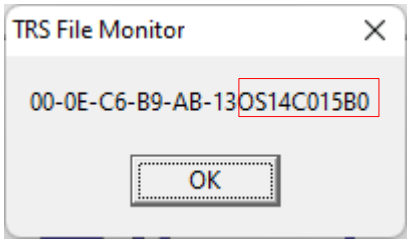
- It is specially designed for client-side or server-side hardware authentication for Windows Remote Desktop Connection login to prevent user passwords from being hacked, and an additional layer of stricter protection makes mobile office or remote login more secure. As described in Section 2.4.
- If TRS File Monitor is not installed on the client side, such as logging in with the mobile RDC APP, the server-side hardware verification will be performed automatically.
- If TRS File Monitor is installed on the client side, it will be automatically verified without entering the verification code, but if the verification fails, the server-side hardware verification will also be activated. You can log out automatically after 30 seconds and then log in again.
- The clipboard function of Windows Remote Desktop Connection must be checked to perform client hardware authentication. as shown in the figure



- Client or Server hardware TRS Verification Key can change the Label of Hard Disk C: disk at any time to change a part of TRS Verification Key to increase security. as shown in the figure.

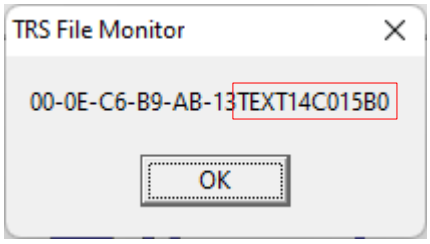
Step1 : Before changing, open cmd as a system administrator to query the current label value, enter: label

Step2 : And open the machine code in the way of chapter 2.4.1



Step3 : Enter the name of the volume to be changed: TEXT (example)

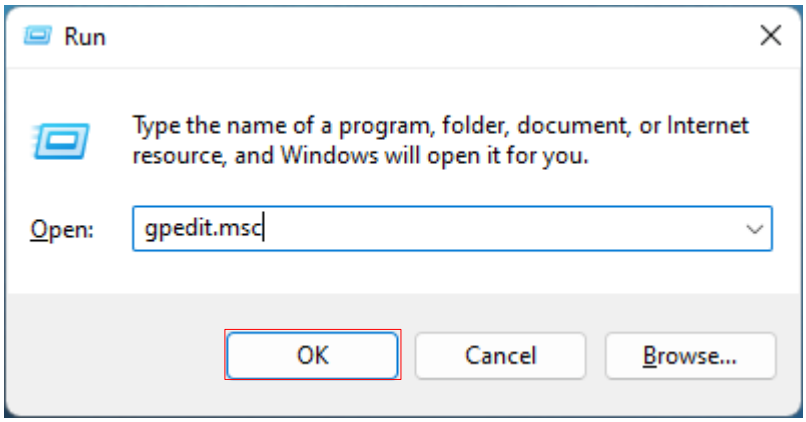
Step4 : Query the corrected key in the way of Section 2.4.1



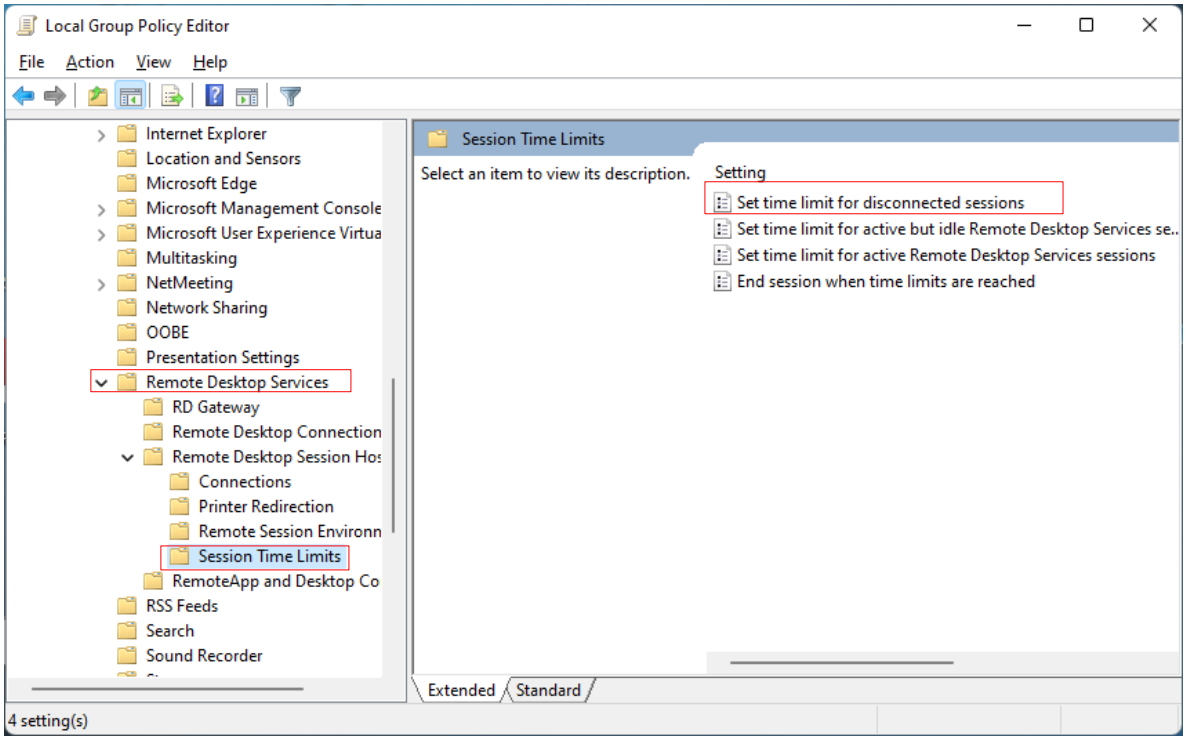
- When the verification function is enabled on the server side, if you forget the TRS Key and the system cannot log in, you can enter the console of the local machine to obtain or set the TRS Verification Key. See chapter 2.4.1 for details.

- When the RDC is disconnected, it must be set to log out immediately, as shown in the figure

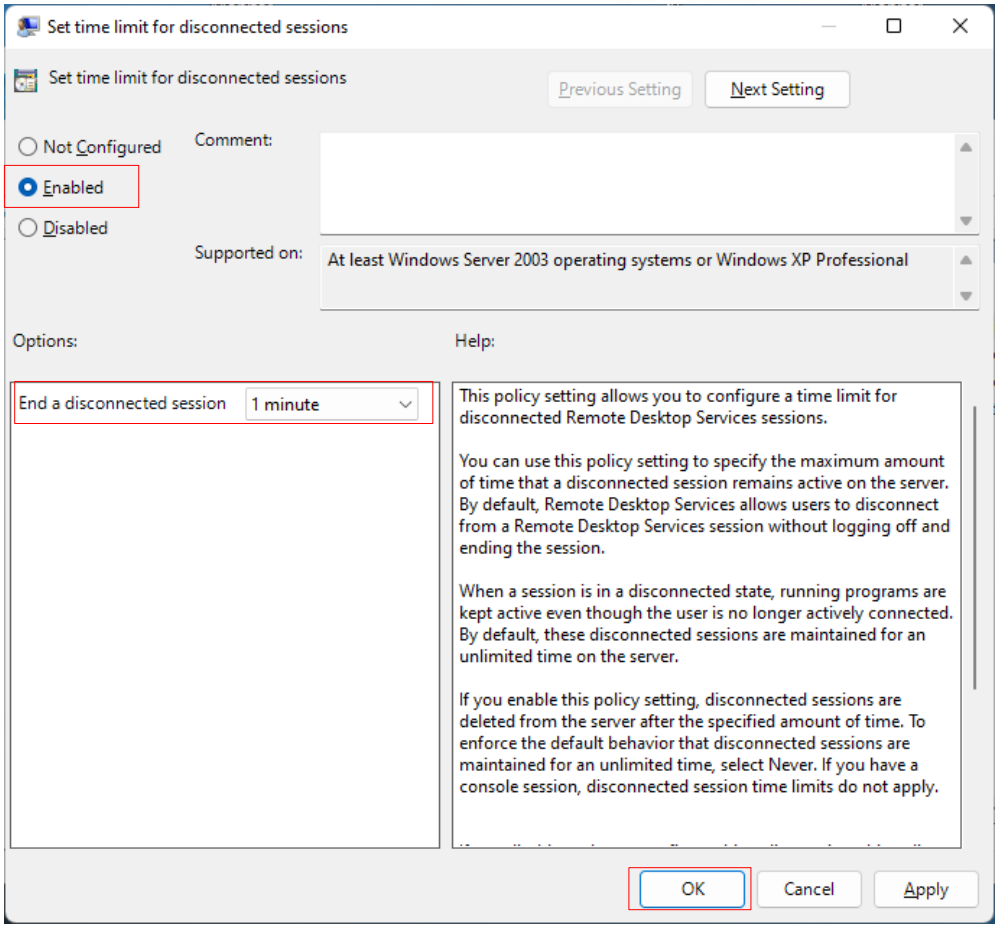
Step1 : First open the "Group Object Principle Editor" and enter gpedit.msc



Step2 : Find Local Computer Policy / User Configuration / Administrative Templates / Windows Components / Remote Desktop Services (Terminal Services) / Remote Desktop Sessions Host/ Session Time Limits, select "Set Time Limit for Disconnected Sessions"



Step3 : Set the time limit for the disconnected work phase, check Enabled, and set the number of minutes (selected according to the user's situation)



- Server hardware TRS Verification Key verification code must be input with dynamic value to increase security。

3.15 How to use functions such as copy (Ctrl+C) and cut and paste (Ctrl+V) to enter the server-side verification code?

When the server-side verification screen appears, switch to the client-side, copy (Ctrl+C) the string, then switch to the server-side verification screen, and paste (Ctrl+V) the string in the verification field

3.16 Why doesn't the cut-and-paste function of Remote Desktop Connection work?

When the Verification function is enabled, you must log in for verification before the clipping function can be used normally。

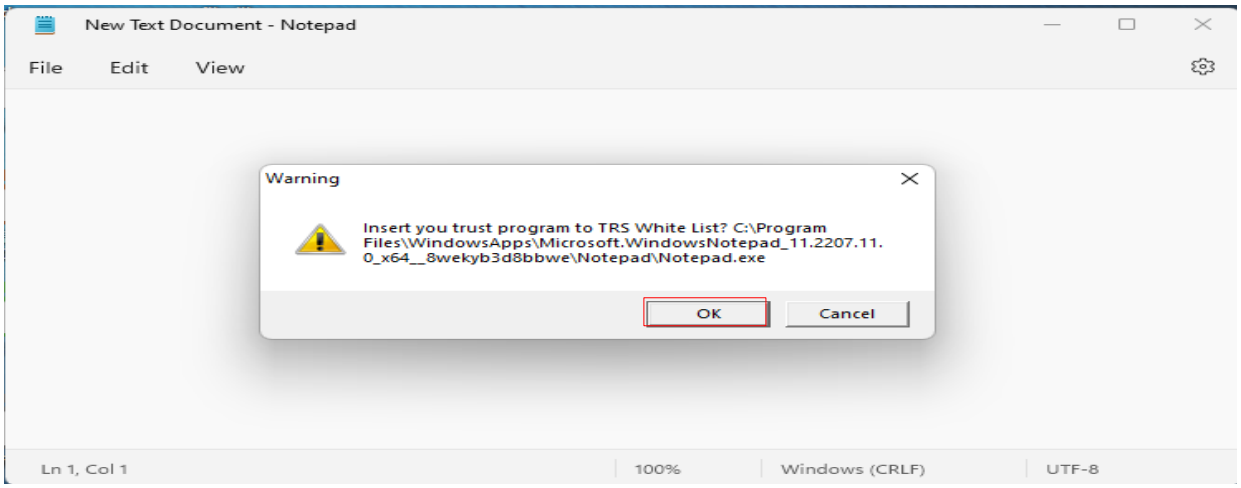
3.17 When a legitimate program was opened, it was mistakenly identified as ransomware, a warning message appeared, and the program could not be used normally?

You can go to the isolation area (Isolation) to restore the program (Restore) to use it normally, as detailed in chapter 2.5。

3.18 The message of whether to add the program to the White List suddenly appears, should it be

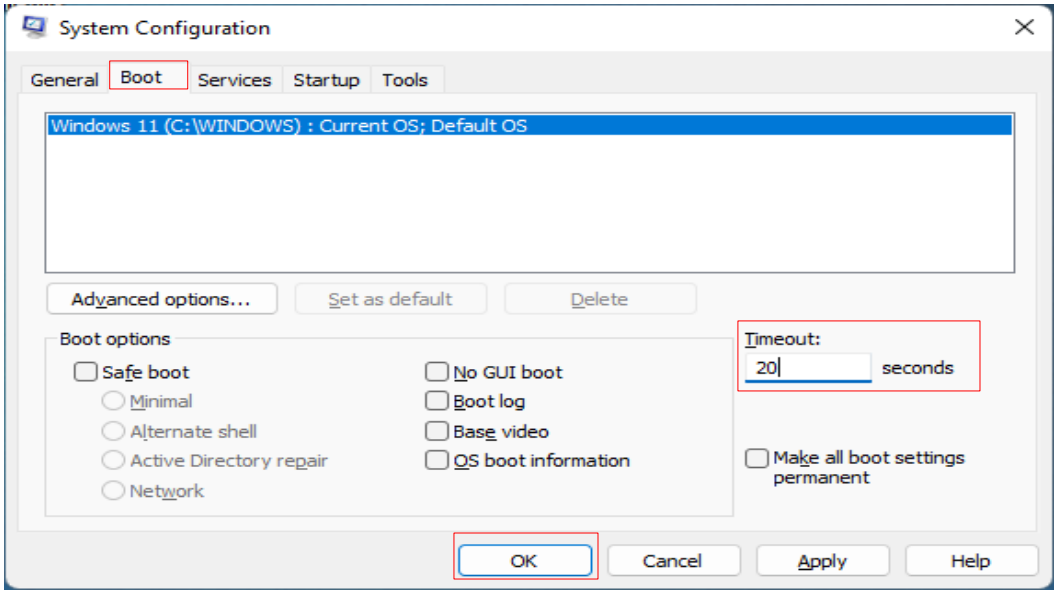
added?

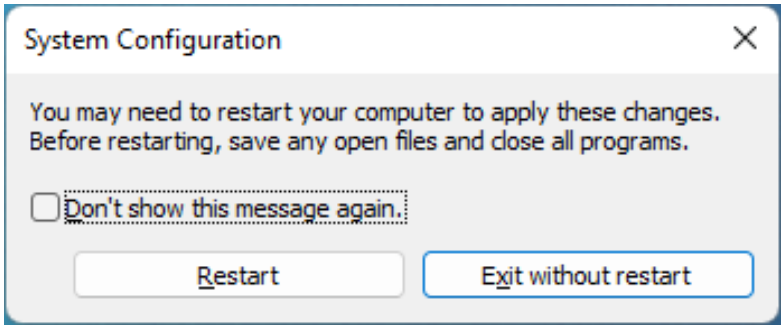
If the message appears immediately during the process of manually opening the program, for example, when the user opens the notepad, this message appears, and you can safely add the notepad to the White List to avoid the program being forced to end during the execution process, as shown in the figure

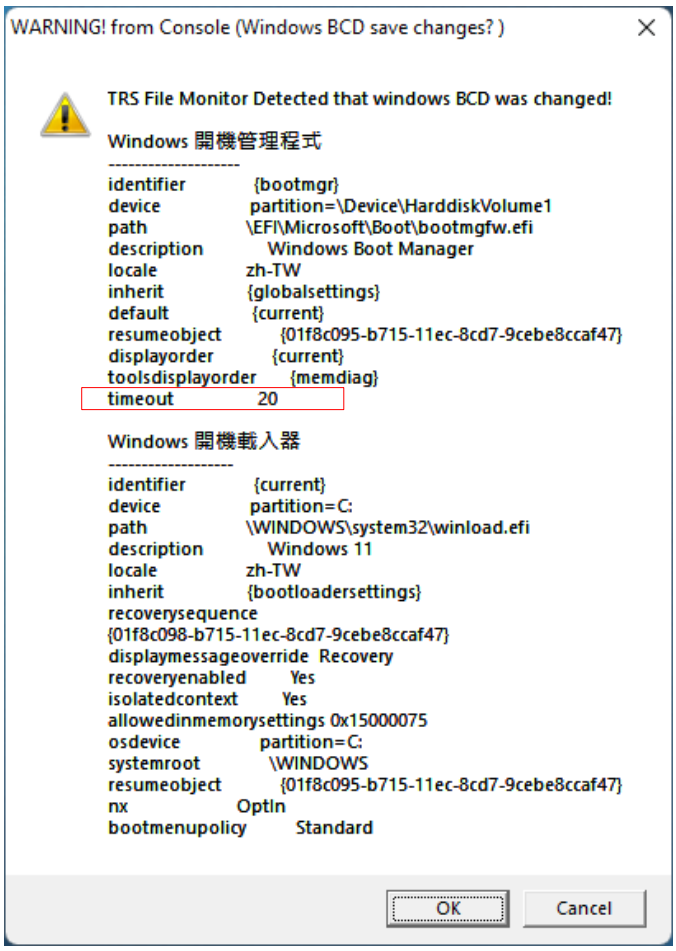


3.19 Executing Msconfig.exe to modify boot data is invalid?

Because the following information has not been confirmed, as shown in the figure







3.20 Is there a risk of capital leakage when using TRS File Monitor?

Unlike other software that will send back various information on the user's computer, TRS File Monitor does not connect to any external host, completely eliminating the risk of personal information leakage (even if it is allowed by the user, it is also possible to send back the suspicious extortion records to assist in interpretation. Of course), follow the EU norms to prevent personal information leakage.

3.21 How to Build an Environment Against Ransomware?

- Good backup and restore (instant/batch/offsite)
  Make reasonable investment in equipment according to acceptable risk.
- Implement information security policy management (windows settings/authority management/firewall management)
  1. Windows settings: enable UAC (User Account Control), etc.
  2. Authority management: Try not to log in with system administrator authority.
  3. Firewall: Regularly check hardware and software firewalls, control DNS, IP and Port, etc.
- Install TRS File Monitor-Anti Ransomware
  Able to prevent firewall (port 135/139/445), PSEXEC, PowerShell, BCD (Boot Config Database), API Hook, Remote Desktop Connection, DOS Command (Regedit, WMIC...) and suspicious ransomware, etc. , do effective protection.