TRS File Monitor

User Guide





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.	Star	t TRS File	Monitor	3
	1.1	TRS Fi	ile Monitor installation	3
	1.2	Auton	natically add to the White List	4
	1.3	Warni	ing	4
	1.4	Popup	o window	5
	1.5	TRS Fi	ile Monitor operation	5
2.	TRS	File Mon	itor button function	6
	2.1	Unins	tall	6
	2.2	Stop		6
	2.3	White	e List	6
		2.3.1	Adding Frequently Used Programs from administrator	7
		2.3.2	The user adds the program from the file path	7
		2.3.3	Add to the White List from sequences detected as suspicious programs	7
	2.4	Verific	cation	8
		2.4.1	Checking the machine code	8
		2.4.2	Enable hardware verification	8
		2.4.3	Random number verification code	9
	2.5	Isolati	ion	9
		2.5.1	Restore	9
		2.5.2	Delete	9
	2.6	Hide		10
	2.7	About	t	10
		2.7.1	Release information	10
		2.7.2	Contact the TRS File Monitor team	11
		2.7.3	Detection report	11
		2.7.4	Send report to TRS File Monitor development team	12

3. Fi	requently asked questions	13
	3.1 Why Install TRS File Monitor?	13
	3.2 Differences between the free trial version and the paid version of TRS File Monitor.	13
	3.3 When installing a new program, it was blocked by TRS File Monitor, which made the installation	
	impossible	13
	3.4 TRS File Monitor was tested to block the following ransomware	14
	3.5 Computer specifications for installing TRS File Monitor	14
	3.6 UAC (User Account Control) is strongly recommended	14
	3.7 Why am I still being asked to enter the machine code even though hardware verification is turned	d
	on?	16
	3.8 Sever has installed TRS File Monitor, but it is not installed on this machine. Why does it log out a	nd
	jump back to this machine when entering random numbers?	16
	3.9 Can't see the TRS File Monitor Icon in the Windows taskbar?	16
	3.10 Press Stop of TRS File Monitor to stop monitoring, will it also stop the ransomware prevention	
	function?	16
	3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end	1?
	3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end	1? 16
	3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end3.12 Does the ransomware prevention feature also stop when the system is logged out?	d? 16 16
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out? 3.13 How do I know if a suspicious ransomware behavior is detected? 	d? 16 16 17
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out? 3.13 How do I know if a suspicious ransomware behavior is detected?	d? 16 16 17 17
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	1? 16 16 17 17
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out? 3.13 How do I know if a suspicious ransomware behavior is detected? 3.14 What is the verification function for? 3.15 How to use functions such as copy (Ctrl+C) and cut and paste (Ctrl+V) to enter the server-side verification code?	 16 16 17 17 20
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 16 16 17 17 20 20 20
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 J? 16 16 17 17 20 20 g
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 J? 16 16 17 17 20 20 g 20 20
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out? 3.13 How do I know if a suspicious ransomware behavior is detected? 3.14 What is the verification function for?	 16 16 17 17 20 20 g 20 20
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 1? 16 16 17 17 20 20 g 20 20 20 20 20 20 20
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 j? 16 17 17 20 20 g 20 z0 <l< td=""></l<>
	 3.11 Does the ransomware prevention feature also stop when pressed to end or when forced to end 3.12 Does the ransomware prevention feature also stop when the system is logged out?	 d? 16 17 17 20 20 g 20 20 20 21 22

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

TRS File Monitor						- 0 X
🕀 New 🗸		Sort 🗸 🗮 View 🗸				
\leftarrow \rightarrow \checkmark \uparrow	> TRS File Monitor				~ C	Search TRS File Monitor
V 🔶 Quick access	Name	Date modified	Туре	Size		
Deskton	S ChkTRSFileMonitor	2/15/2022 1:28 PM	Windows Batch File	1 KB		
↓ Downloads 🖈	S FileM Warning		11P 1 P. 1 P.	×		
📑 Documents 🖈	Read Insert you trust program fr	om Task Manager to TRS W	hite List? C:\Windows\Sys	stem32\smss.exe		
🔀 Pictures 🖈		3				
🚅 G:\ 🛷	TRS \	<u>No</u> <u>A</u> bor	Yes to <u>A</u> ll			
Adobe_CS6	TRS TEMP.K	9/13/2020 2:21 PM	K File	0 KB		
System32		3/5/2021 8:32 AM	TMP File	1 KB		
늘 TFM	TRSFileService	2/5/2021 3:15 PM	Application	914 KB		
늘 請勿破-行程規i	TRSMsg	10/8/2020 3:17 PM	Application	911 KB		
> 🌰 OneDrive	3 TRSWebSite	1/19/2021 11:08 AM	Windows Batch File	2 KB		
This PC This I item selected	3.80 MB					

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.

🚡 TRS File Monitor					
Ransomware behavior is detected. If the program you trust is closed, it is strongly recommended to add to the [TRS White List]. Opening [TRS Isolation] can help you restore deleted programs.					
Close					

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.



🖉 TRS File Monitor - Anti Ransomware —	×									
TRS File Monitor										
7										
Thinstall I Stop White List Verification I Isolation Hide About										
The system window is closed, User:= ,Domain:=, ExePath:=, ProcessID:=0										
2022/09/13 10:32:05>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Site Characteristics Database\LOG 2022/09/13 10:32:05>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Sync Data\LevelDBL\OG 2022/09/13 10:32:05>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Extension Script\LOG 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Extension Script\LOG 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Temp\3909cdd5-4ea4-4626-b00a-71a728cafcbb.tmp 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\f_001fb3 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\f_001fb3 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\f_001fb3 2022/09/13 10:32:05>CreateFile:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\f_001fb3 2022/09/13 10:32:06>Modifiltem:C:\Windows\Prefetch\CHROME_EXE_53:49D2DF.pf 2022/09/13 10:32:06>Modifiltem:C:\Windows\Prefetch\CHROME_EXE_53:49D2DF.pf 2022/09/13 10:32:06>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:07>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:08>Modifiltem:C:\Users\TRS\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 2022/09/13 10:32:08>Mo	ppl 									

2. TRS File Monitor button function

2.1 Uninstall

After clicking the button, the program will be uninstalled.

TRS File Monitor - Anti Ransomware								
	TRS File Monitor							
Tuninstall	Stop	💭 White List	% Verification	會 Isolation	Hide	? About		

2.2 Stop

When the button is clicked, the detection stops.

TRS File Monitor - Anti Ransomware								
	TRS File Monitor							
🚡 Uninstall	Tuninstall Stop White List Verification Isolation Hide ? About							
2.3 White List								
	TRS File Monitor - Anti Ransomware	_ D X						
	TRS File Monitor							
ᡖ Uninstall	Stop Image: Stop	? About						

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 \circ 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.

TRS File Monitor - Anti Ransomware							
	TRS File Monitor						
🚪 Uninstall	Stop	White List	& Verification	壶 Isolation	🗟 Hide	? About	

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.

	TRS Verification Key		_ □	x			
TRS Verification Key							
≠i Insert ±i Delete ☞i Find Fin	nd						
Client Key							
✓ Verify Client Key							
[TRS Verification Key] 00-50-56-C0-00-01 OSA8F98177=ok 00-15-5D-BC-B2-62A00A9A92=ok 00-0E-C6-B9-AB-EEOS8C03CB89=ok 00-E0-4C-33-07-FFOS4666E6D0=ok 2C-56-DC-72-75-E9Windows20BB0982=ok 34-97-F6-83-92-35Windows78BE7C346=ok 34-97-F6-82-D7-1EWindows78DE73AA=ok A8-A1-59-4F-D3-3BF6182293=ok 00-50-56-C0-0000SA8E08177=ok	TRS File Monitor X 34-97-F6-5A-69-50A00A9A92 OK						
04-D9-F5-B9-10-C0OS7EC8FA66=ok 00-0C-29-FC-B8-6ATRS680C5789F=ok BC-AE-C60-A4-4C-39-06-0360EB27DE=ok 38-00-25-3C-02-D0OS4666E6D0=ok				>			

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.

TRS File Monitor - Anti Ransomware					
	TRS File Monitor				
🚡 Uninstall	Stop Stop White List & Verification Hide	? About			

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.

🖉 TRS File Monitor - Anti Ransomware								
	TRS File Monitor							
🚪 Uninstall	Stop	🗒 White List	% Verification	✤ Isolation	🗟 Hide	? About		

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.

TRS File Monitor - Anti Ransomware						_ _ ×	
	TRS File Monitor						
Tuninstall	Stop	C White List	% Verification		🗟 Hide	? About	

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.



	TRS_Readm	ne - Notepad	ł									_		×
File	Edit	View												ŝ
Us Us 20 20 20 20 20 20 20	er:=S` er:=S` 22/09 22/09 22/09 22/09 22/09 22/09	YSTÉM YSTEM /01 09 /01 09 /01 09 /01 09 /01 09 /01 09	,Domain: ,Domain: 2:48:19>C 2:48:48>C 2:48:49>C 2:48:52>C 2:53:01>C 2:53:02>C	=NT reat reat reat reat reat reat	AUTHOR AUTHOR eFile eFile eFile eFile eFile eFile	RITY, RITY, :C: \P :C: \P :C: \P :C: \P :C: \P :C: \P	ExeF ExeF rogra rogra rogra rogra rogra	Path: Path: umDat umDat umDat umDat umDat	=C:\P =C:\P a\ASU a\ASU a\ASU a\ASU a\ASU a\ASU	rogram rogram S\ASUS S\ASUS S\ASUS S\ASUS S\ASUS S\ASUS	Files Files System System System System System	(x86) (x86) Cont Cont Cont Cont Cont	God God rol rol rol rol rol rol	gle' Inte Inte Inte Inte Inte Inte Inte
Ln 1	, Col 1								100%	Wind	ows (CRLF)	UT	F-8 with	n BOM

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.

XThere is no risk of personal information leakage in this content

X		
or/	Information	Х
i. itio: wa boc	Mail is sended.	
ter'	ОК	
		x OT/ Information tio: wa boc tet' OK

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	\checkmark	\checkmark		
Personal service	×	\checkmark		
Customized service	×	✓ (such as <u>3.21</u>)		
Authorization	×	\checkmark		
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 <u>2.2</u>) 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 、 WannaCr ypt 、 Petya 、 Bad Rabbit, Helps users to perform normally in a safe environment.

- 3.5 <u>Computer specifications for installing TRS File Monitor.</u>
 - 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.

 Control Panel

 All Apps Documents Web More →

 0
 ♥ P ····

 Best match

 Control Panel

 Mapp

 App

 Apps

 Control Panel

 Apps

 Control Panel

Step1 : Type in the computer search tool - console panel

Step2 : Click on [User Accounts]

🔛 Control Panel		– 🗆 X
$\leftarrow \rightarrow $ $\checkmark $ \uparrow	🚾 > Control Panel	 ✓ Č Search Control Panel
	Adjust your computer's settings	View by: Category 🔻
	System and Security Review your computer's status Save backup copies of your files with File History	User Accounts
	Network and Internet	Appearance and Personalization
	View network status and tasks Hardware and Sound	Clock and Region Change date, time, or number formats
	View devices and printers Add a device Adjust commonly used mobility settings	Ease of Access Let Windows suggest settings Optimize visual display
	Programs Uninstall a program	

Step3 : Select[User Accounts]again



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

8	User Accounts					-	- 0	J	×
	$\leftarrow \rightarrow \checkmark \uparrow$	🍇 > Contro	Panel > User Accounts > User Accounts		C C	Search Control P	anel	م	S
	Control Panel Home	e	Make changes to your user account						?
	Manage your creder Create a password re	ntials eset disk	Make changes to my account in PC settings						
	Manage your file en certificates	cryption	 Change your account name Change your account type 						
4	 Configure advanced profile properties 	l user	•						
	Change my environ variables	ment	 Manage another account 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 <u>3.14</u>

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 <u>1.4</u>
- 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 <u>2.7.3</u>.

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 <u>2.4</u>.
- 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

Nemote I	Desktop Connection		—		×
A	Remote Deskto Connection	p			
General Dis	splay Local Resources Ex	perience	Advanced		
Remote aut	dio Configure remote audio setti <u>S</u> ettings	ings.			
Keyboard	Apply Windows <u>k</u> ey combine Only when using the full sc Example: ALT+TAB	ations: reen		~	
Local devic	es and resources Choose the devices and res your remote session. Printers <u>M</u> ore	cources that	: you want t ard	o use in	
Hide Opti	ons		onnect	<u>H</u> e	lp

• 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

TRS File Monitor	\times
00-0E-C6-B9-AB-130514C015	B0
ОК	





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

TRS File Monitor	×
00-0E-C6-B9-AB-13TEXT14C015	B0
ОК	

• 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.

Copyright (C) 2022 Team Rise System Co., Ltd.

 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

💷 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	gpedit.msc 🗸 🗸
	OK Cancel <u>B</u> rowse

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)

Set time limit for disconnected sessions Previous Setting Next Setting Next Setting
Set time limit for disconnected sessions Previous Setting Not Configured Comment: Enabled Image: Set time limit for disconnected sessions
Not Configured Comment: • Enabled
() Disabled
Supported on: At least Windows Server 2003 operating systems or Windows XP Professional
· · · · · · · · · · · · · · · · · · ·
Options: Help:
End a disconnected session 1 minute This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session. When a session is in a disconnected state, running programs are kep tactive even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server. If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

 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 <u>Why doesn't the cut-and-paste function of Remote Desktop Connection work?</u>
```

When the Verification function is enabled, you must log in for verification before the clipping

function can be used normally. $\,\circ\,$

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

	New Text D	ocument	: - Notepad	_		\times
File	Edit	View				ණ
			Warning × Insert you trust program to TRS White List? C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2207.11. 0_x648wekyb3d8bbwe\Notepad.vec OK Cancel			
Ln 1	I, Col 1		100% Windows (CRLF)	UTF-8	3	

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

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

System Configuration		
eneral Boot Services Startup	Tools	
Windows 11 (C:\WINDOWS) : Currer	it OS; Default OS	
Advanced options Set as	s default <u>D</u> elete	
Boot options		Timeout:
Sa <u>f</u> e boot	No GUI boot	20 seconds
○ Minimal	Boot log	
Alternate shell	Bas <u>e</u> video	
 Active Directory repair 	OS boot information	Make all boot settings
○ Net <u>w</u> ork		permanent
	OK Cano	el <u>A</u> pply Help

System Configuration	×		
You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs.			
Don't show this message again.			
Restart Exit without restart			

WARNING	i! from Console (Windows BCD save changes?)	×
<u> </u>	TRS File Monitor Detected that windows BCD was changed! Windows 開機管理程式	
	identifier {bootmgr} device partition=\Device\HarddiskVolume1 path \EFI\Microsoft\Boot\bootmgfw.efi description Windows Boot Manager locale zh-TW inherit {globalsettings} default {current} resumeobject {01f8c095-b715-11ec-8cd7-9cebe8ccaf47} displayorder {memdiag} timeout 20	
	Windows 開機載入器 identifier {current} device partition=C: path \WINDOWS\system32\winload.efi description Windows 11 locale zh-TW inherit {bootloadersettings} recoverysequence {01f8c098-b715-11ec-8cd7-9cebe8ccaf47} displaymessageoverride Recovery recoveryenabled Yes isolatedcontext Yes allowedinmemorysettings 0x15000075 osdevice partition=C: systemroot \WINDOWS resumeobject {01f8c095-b715-11ec-8cd7-9cebe8ccaf47} nx Optin bootmenupolicy Standard	
	OK Cancel	

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.