TRS File Monitor

使用手冊

翊捷資訊股份有限公司

Team Rise System Co., Ltd.

台北市杭州南路1段8-1號4樓

TEL:02-23221622　FAX:02-23223986

統一編號:96943675

DATE：2022/09/12

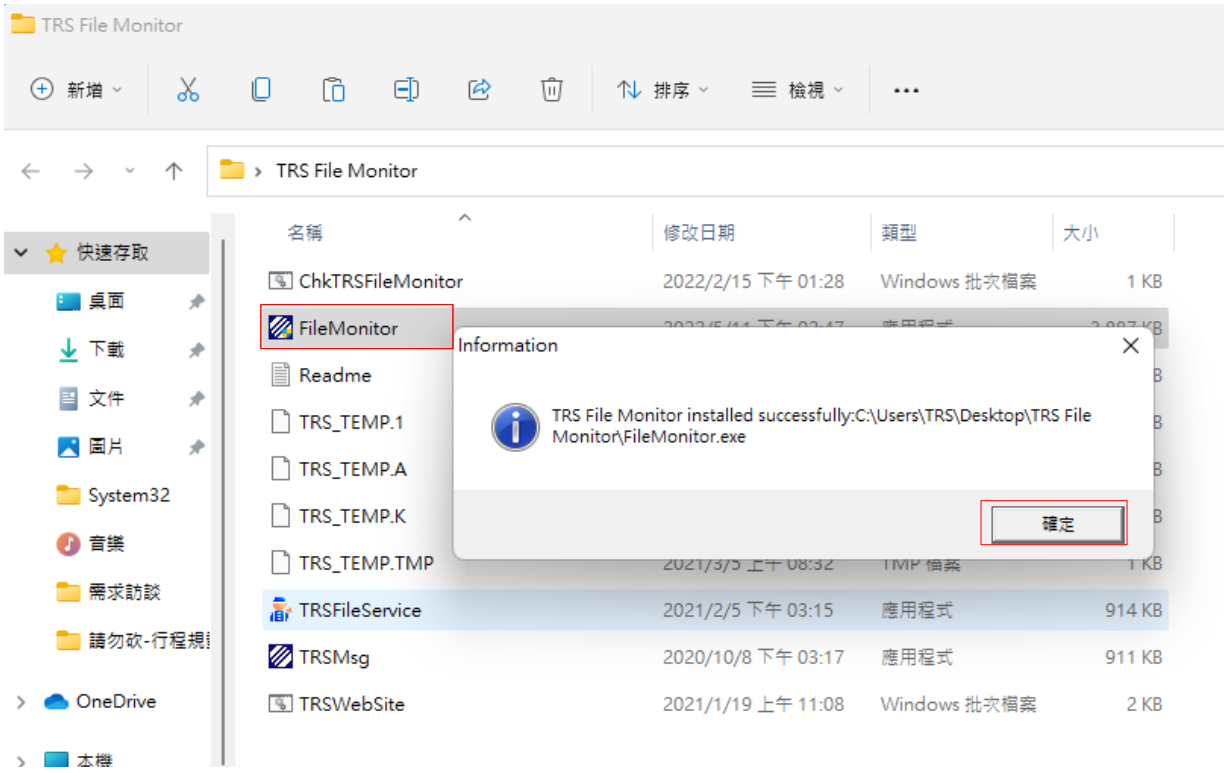
目錄

1. 啟動 TRS File Monitor

1.1 安裝 TRS File Monitor

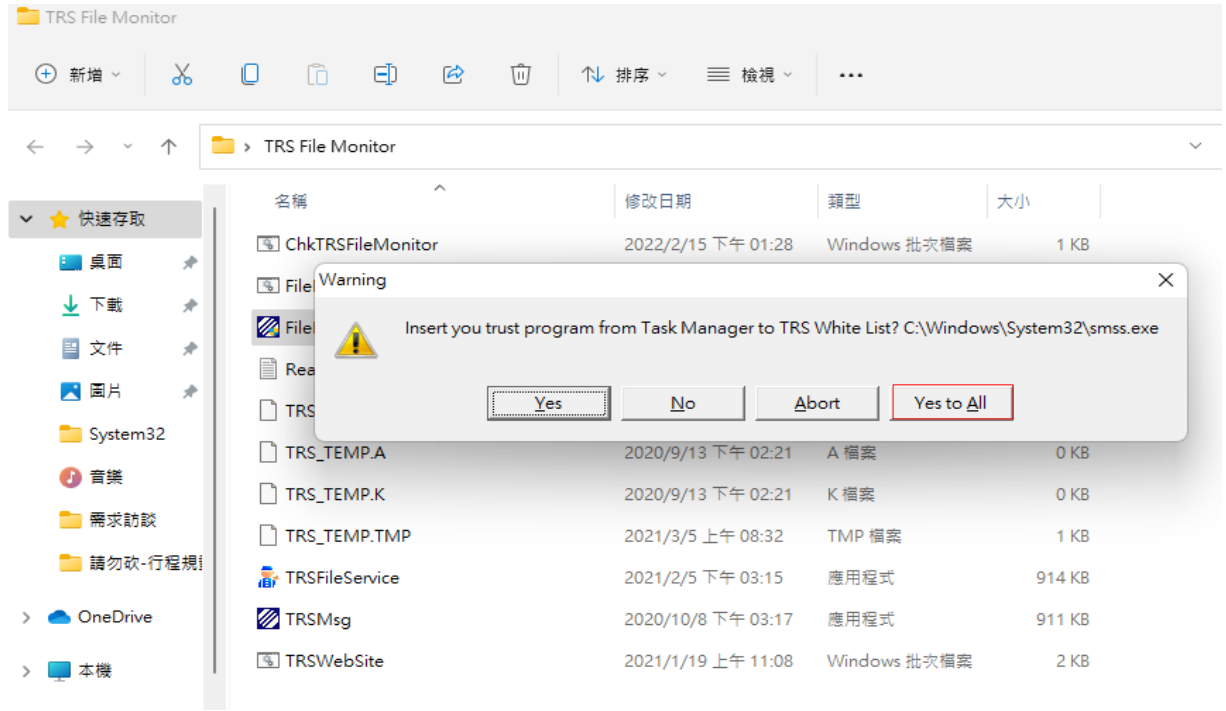
雙擊兩下程式便將會出現使用者帳戶控制之視窗，點選是，即可順利安裝。

安裝成功後，點選確定，TRS File Monitor 正式啟動。



1.2 自動加入白名單

安裝成功後，第一次使用會出現是否將目前開啟中的程式加入白名單，依據工作管理員



按鈕-Yes : 依照訊息視窗中的檔案，逐筆加入白名單。

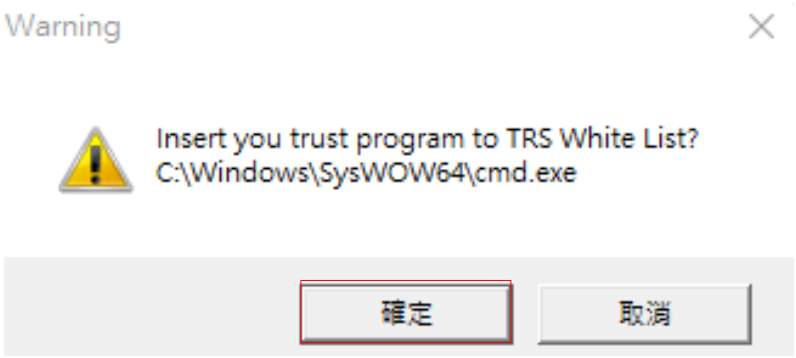
按鈕-No : 依照訊息視窗中的檔案，逐筆不加入白名單。

按鈕-Abort : 全部略過。

按鈕-Yes to All : 全部加入(建議選取)。

1.3 警示訊息

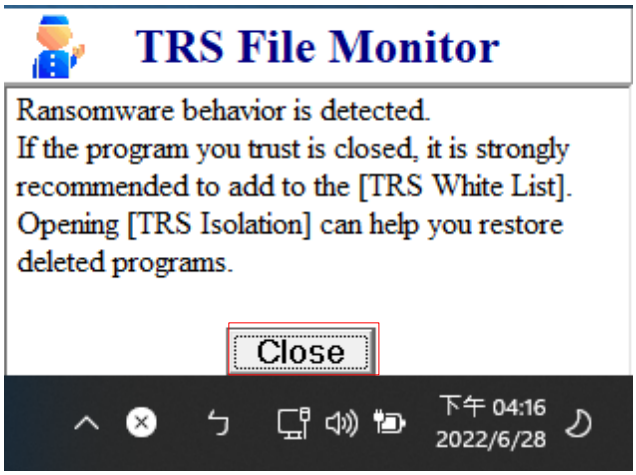
若於 1.2 項目中，未選擇[Yes to All]，則有可能出現下列訊息。



1.4 彈出視窗

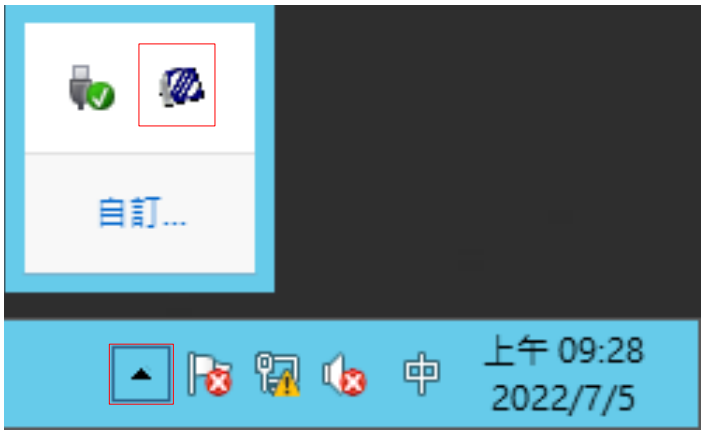
若於 1.2 項目中，未選擇[Yes to All]，亦有可能出現下列訊息。

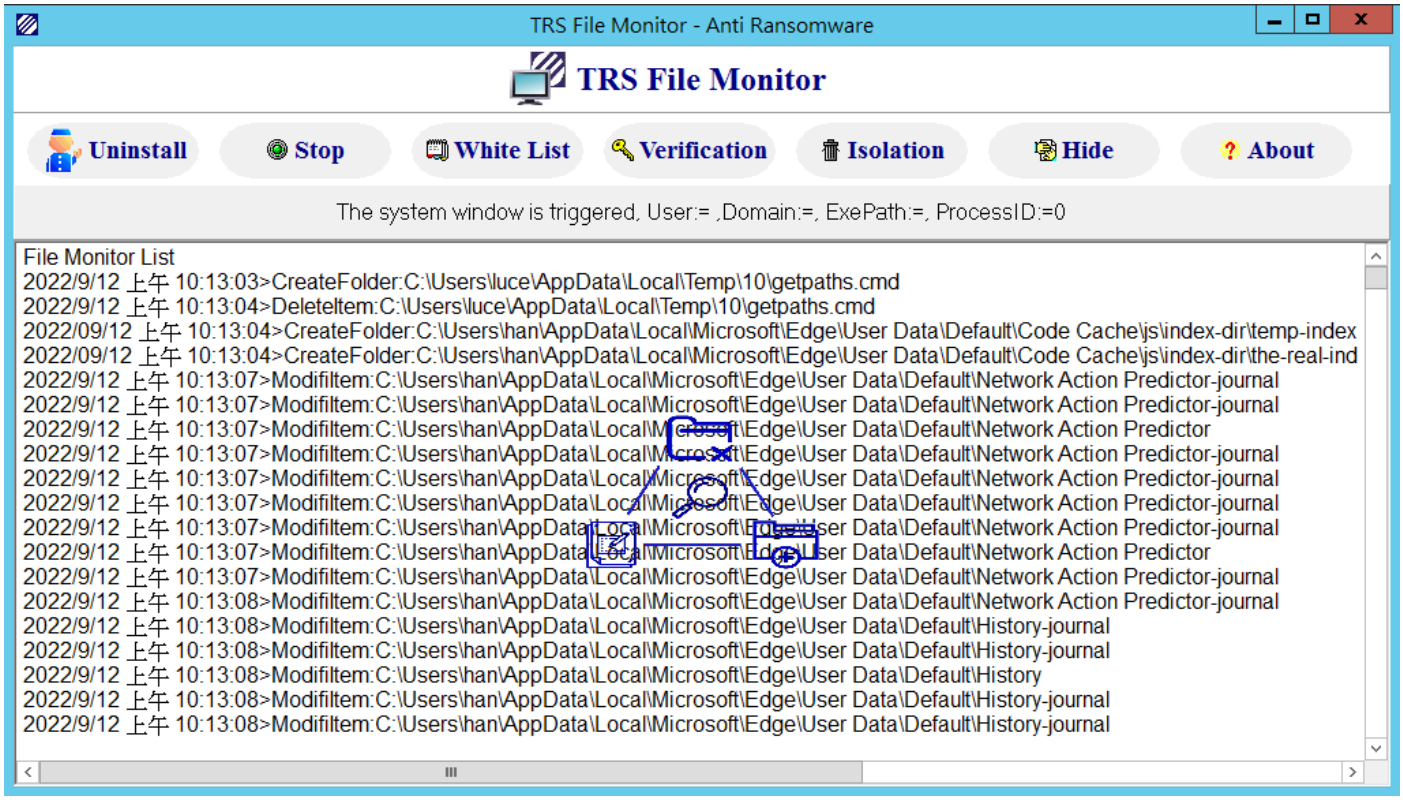
TRS File Monitor 若偵測到可疑行為將於螢幕右下方出現視窗，並將該程式移至隔離區。



1.5 TRS File Monitor 運作畫面

TRS File Monitor 於背景作業執行，並不影響使用者操作，可於工具列中點開圖示，則可看見即時偵測畫面，並使用其他按鈕功能。

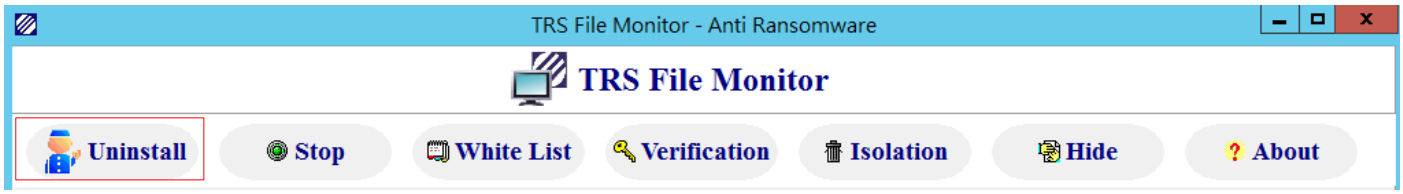




2. TRS File Monitor 按鈕功能

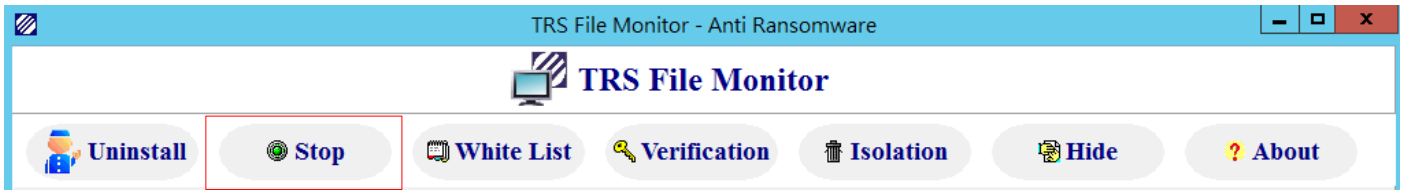
2.1 卸載程式-Uninstall

點選按鈕後，即卸載該程式。

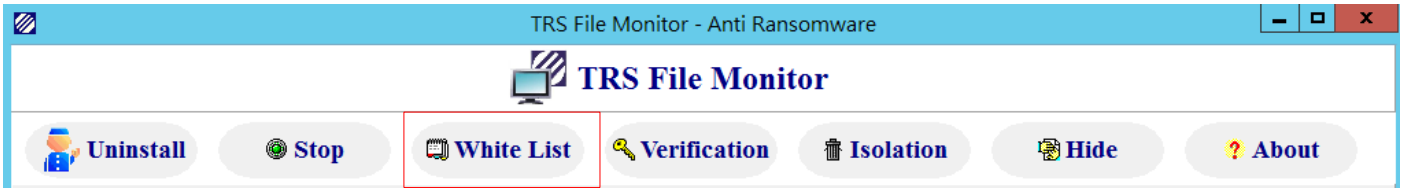


2.2 停止偵測-Stop

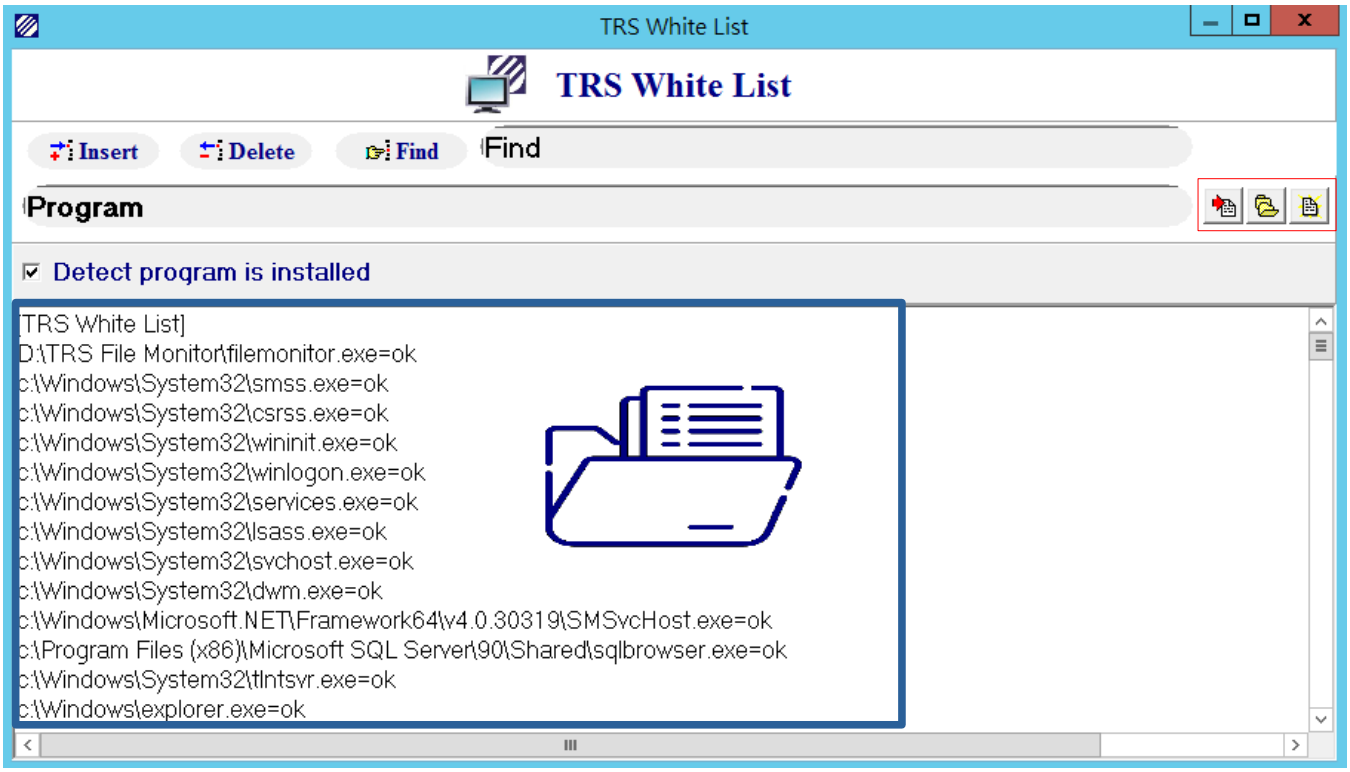
點選按鈕後，即停止偵測。



2.3 白名單-White List

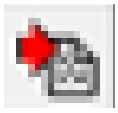


以下有三個方式(紅框處)可將信任程式加入白名單，以避免 TRS File Monitor 誤判，下方藍框則是目前於白名單列表中的程式。



2.3.1 從工作管理員中加入常用程式

TRS File Monitor 會從工作管理員偵測常用的程式，直接加入白名單。

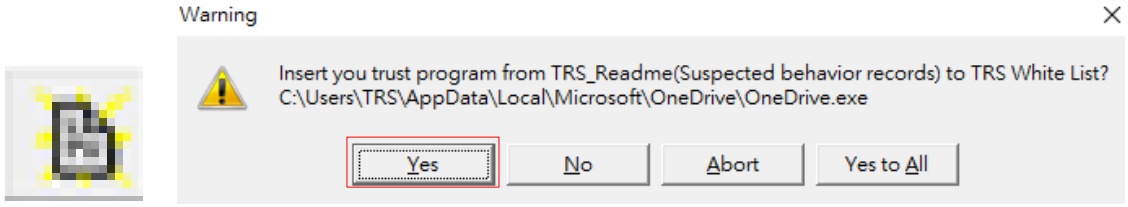


2.3.2 使用者從檔案路徑加入程式

使用者可藉由檔案路徑選擇信任之程式加入白名單。

2.3.3 從被偵測為可疑程式之序列加入白名單

TRS File Monitor 會將可疑程式紀錄至 TRS_Readme.txt 中，使用者點選此按鈕，可加入被偵測為可疑程式之信任的程式，此按鈕會逐筆顯示是否要加入白名單之訊息。



按鈕-Yes : 依照訊息視窗中的檔案，逐筆加入白名單。

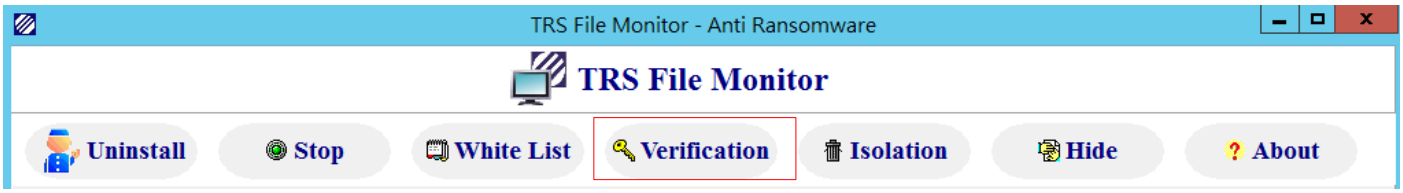
按鈕-No : 依照訊息視窗中的檔案，逐筆不加入白名單。

按鈕-Abort : 全部略過。

按鈕-Yes to All : 全部加入(不建議選取)。

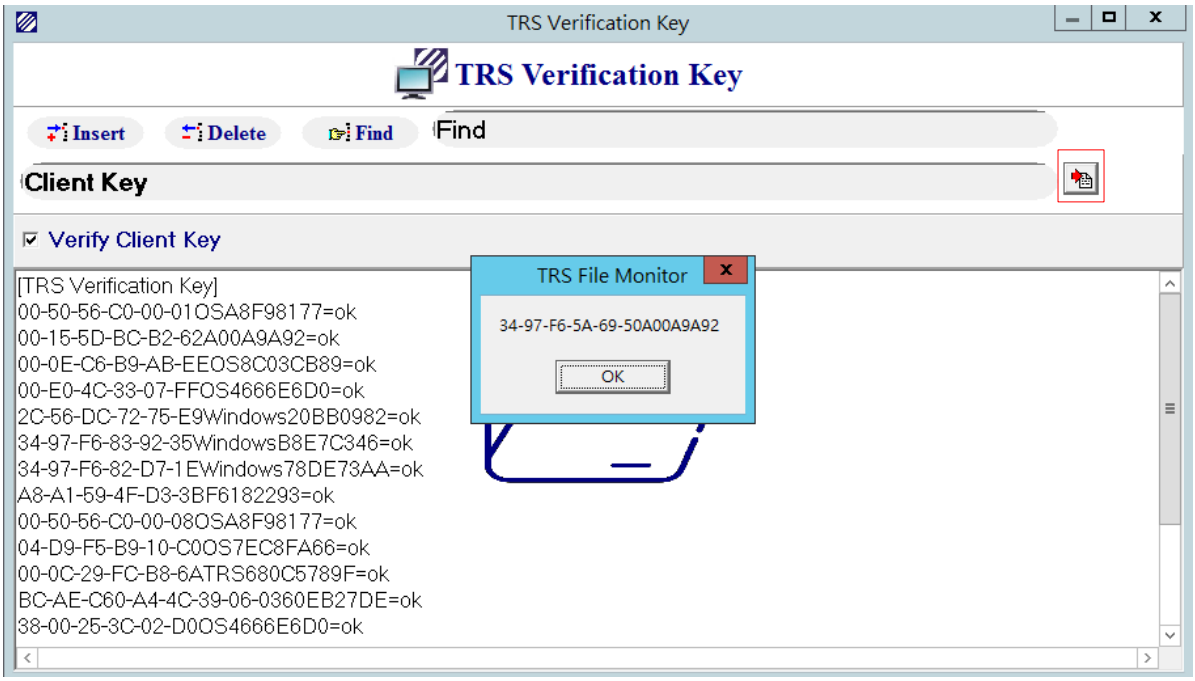
2.4 硬體驗證-Verification

TRS File Monitor 提供多人環境 RDP 登錄時驗證使用，可使用硬體驗證功能加層防護。



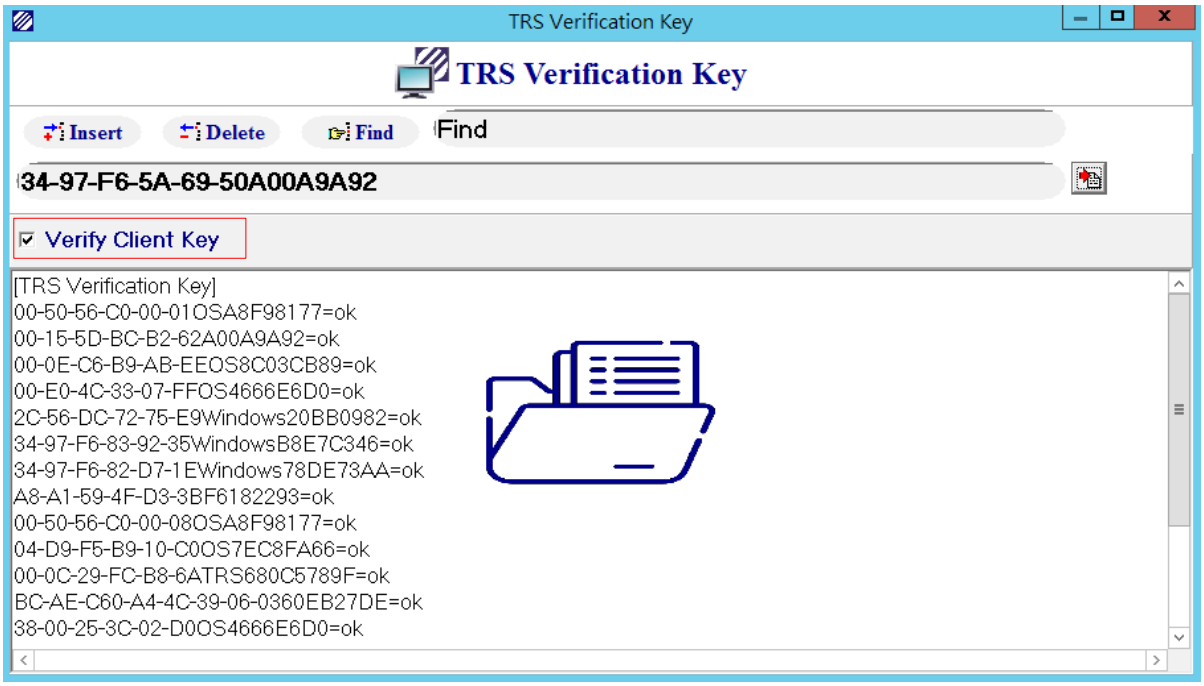
2.4.1 查看本機機碼

點選按鈕後，可顯示本機機碼及複製給系統管理員，以新增至遠端主機。



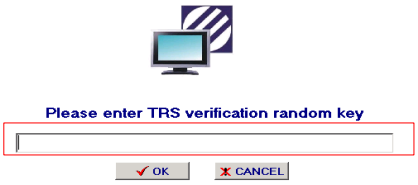
2.4.2 開啟硬體驗證

於遠端主機之 TRS File Monitor 開啟硬體驗證功能(紅色框)，只要欲連線之使用者的主機已新增至名單中，進入遠端主機無須登打驗證碼，即可連線。



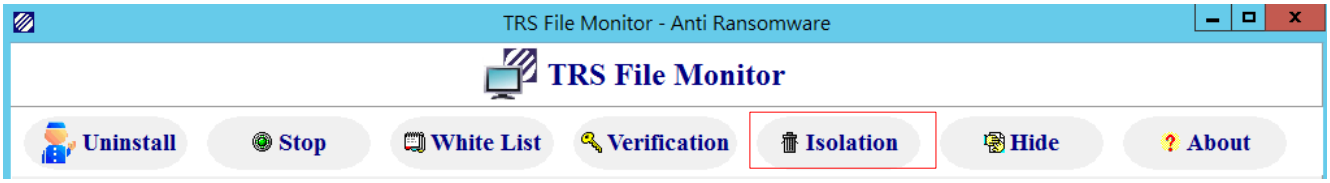
2.4.3 亂數驗證碼

若使用者未安裝 TRS File Monitor，欲連線至遠端主機，除了需輸入原本 RDP 連線之使用者帳密外，也須按照客製化之亂數輸入機碼，才可成功進入遠端主機。



2.5 隔離區-Isolation

當應用程式出現類勒索軟體行為時，將有可能被移至隔離區，以保護使用者作業環境。

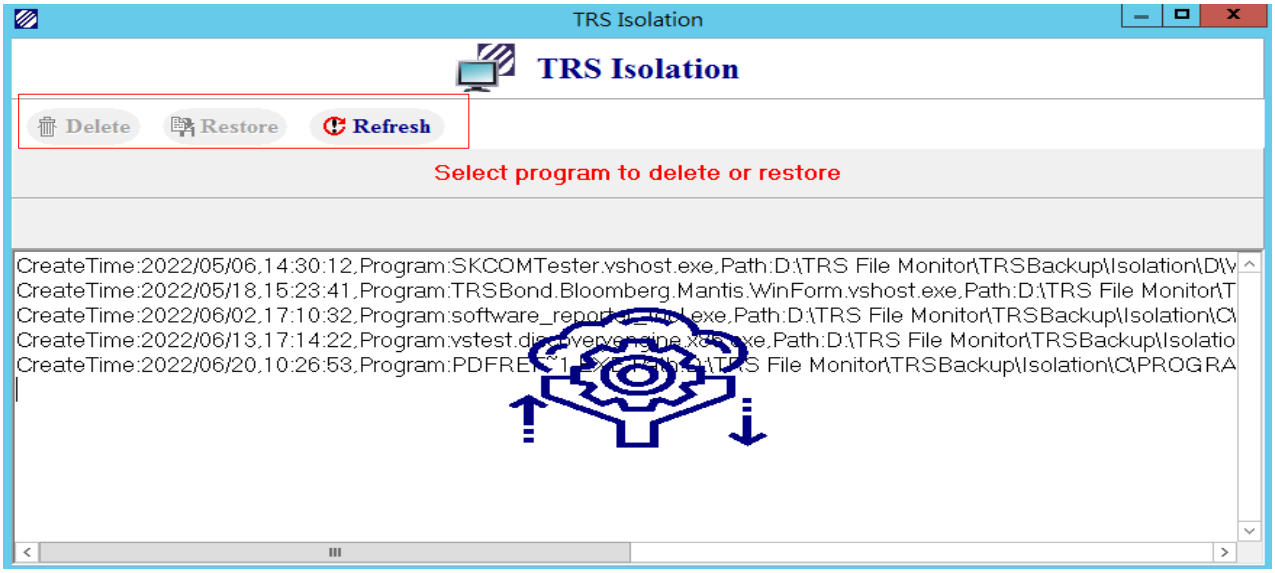


2.5.1 復原程式-Restore

若信任的程式被加入至隔離區導致無法順利執行時，可於隔離區復原，程式將自動加入白名單，並將程式回復到原來安裝的路徑。

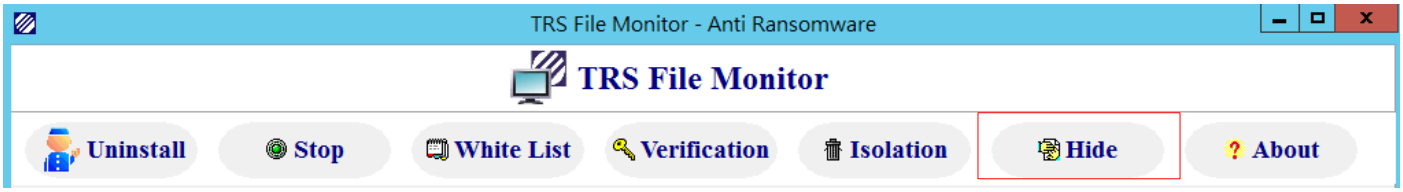
2.5.2 刪除程式-Delete

若隔離區出現可疑程式，可直接透過 TRS File Monitor 刪除該程式。



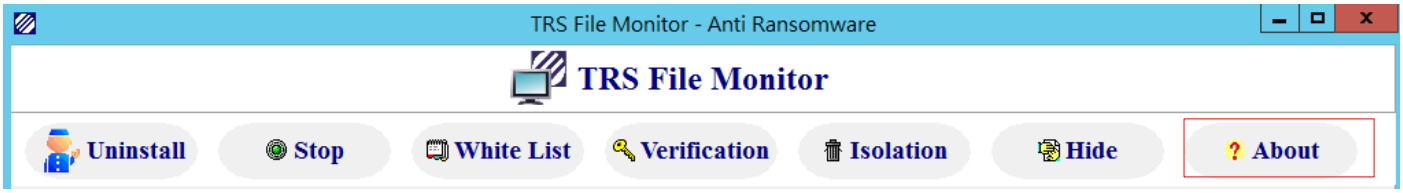
2.6 回到背景作業-Hide

使用者若要隱藏 TRS File Monitor 於桌面，可點選 Hide，讓程式回到背景作業，此動作並不影響偵測進行。



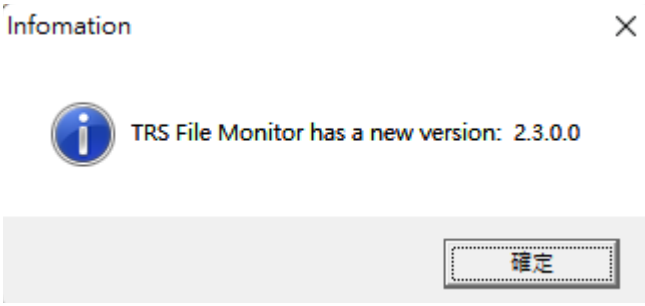
2.7 關於-About

TRS File Monitor 版本資訊位於此頁籤，可提供使用者確認當前是否為最新版本。



2.7.1 版本資訊

若使用者本機之版本非為最新版本，則會跳出提示視窗，且紅框處為試用剩餘天數。

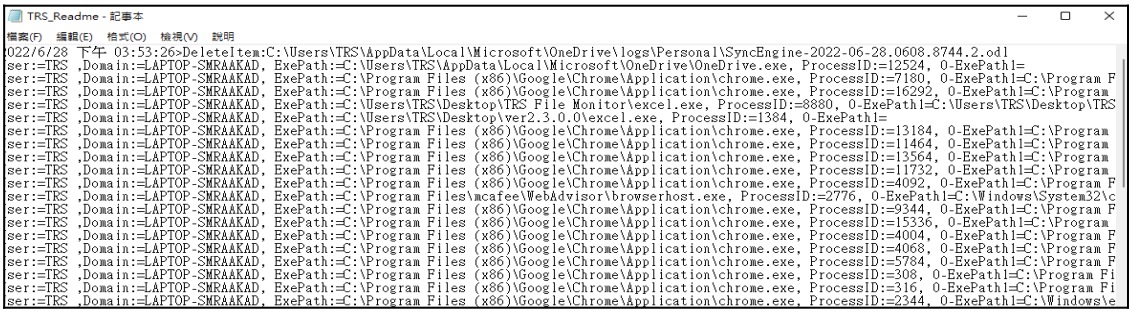


2.7.2 聯繫 TRS File Monitor 開發團隊

可點選網址進入官方網站，藉以更瞭解本產品及聯繫我們。

2.7.3 偵測報告

TRS File Monitor 將會記錄時間與發生疑似勒索行為之檔案列表，可於此按鈕產生清單，提供後續追蹤。



2.7.4 傳送報告給 TRS File Monitor 開發團隊

若對偵測報告有疑惑之時，可藉由此方式傳送報告供開發團隊，進一步與您聯繫。

※此內容無個資外洩之風險

3. 常見問題

3.1 為什麼要安裝 TRS File Monitor ?

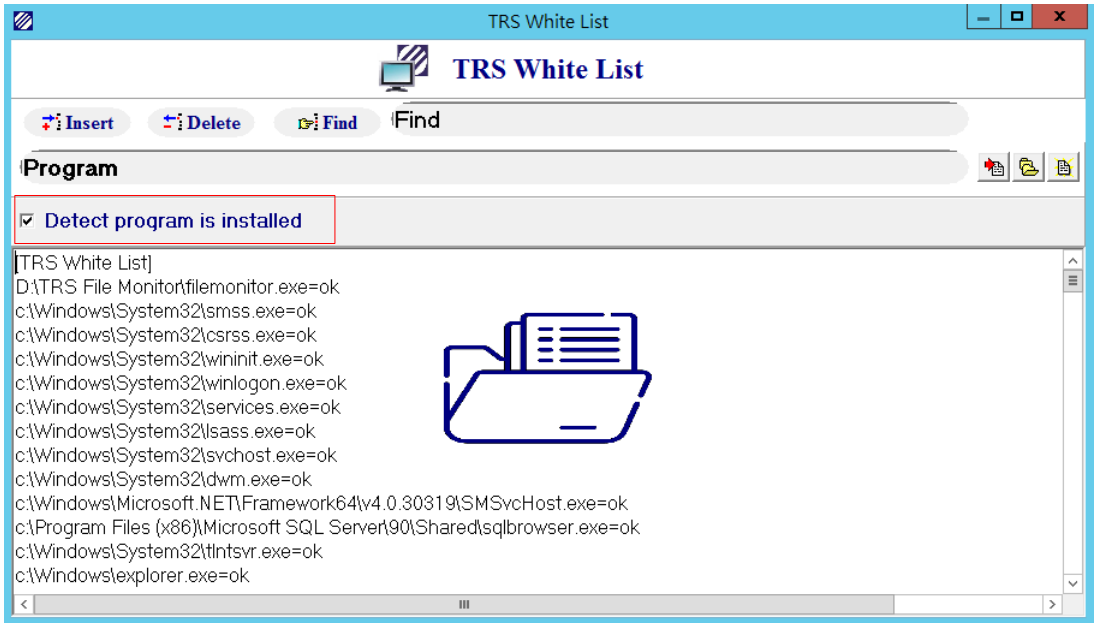
- 以不同於其他防毒或防勒索軟體的觀念與方法，能阻擋全球知名的防毒或防勒索軟體無法阻擋的 Ransomware。
- 偵測到可疑 Ransomware 行為時，及時甚至事先阻擋檔案被變更。
- 從一個平常的建立或更名或刪除檔案行為，即能判斷是否為可疑的 Ransomware。
- 預防 Ransomware 修改 BCD(啟動組態資料庫)。
- 針對 RDP(遠端桌面連線)多一層防護。

3.2 TRS File Monitor 免費試用版與付費版之差異。

功能	免費試用版	付費版
偵測與預防勒索行為	✓	✓
專人服務	×	✓
客製化服務	×	✓ (詳如 3.21)
授權書	×	✓
使用期限	90 天	年費制
不論免費試用或付費版本，資訊安全沒有絕對安全，都需要使用者回饋，讓功能與時俱進。		

3.3 遇到安裝新程式時，被 TRS File Monitor 阻擋，而導致無法順利安裝。

- 於 White List 頁籤中勾選 [Detect Program is installed]，不須結束程式，但為了安全性安裝程式後，記得勾選回 [Detect Program is installed]



- 可以直接點選 Stop 按鈕(如 2.2)，停止偵測，安裝成功後，再點選 Start 恢復偵測。

3.4 TRS File Monitor 經測試，能夠阻擋以下勒索軟體：

Reveton、CryptoLocker、TorrentLocker、CryptoWall、KeRanger、RSA4096、Mischa、WannaCrypt、Petya、Bad Rabbit 等，有助於使用者於安全環境下正常執行。

3.5 安裝 TRS File Monitor 的電腦規格需求。

- Microsoft Windows Server 2008 Standard 以上(包含 x86、x64)
- Microsoft Windows 7 家用進階版以上(包含 x86、x64)
- 強烈建議開啟 UAC(使用者帳戶控制)，詳如 3.6 章節。

3.6 強烈建議開啟 UAC (使用者帳戶控制)。

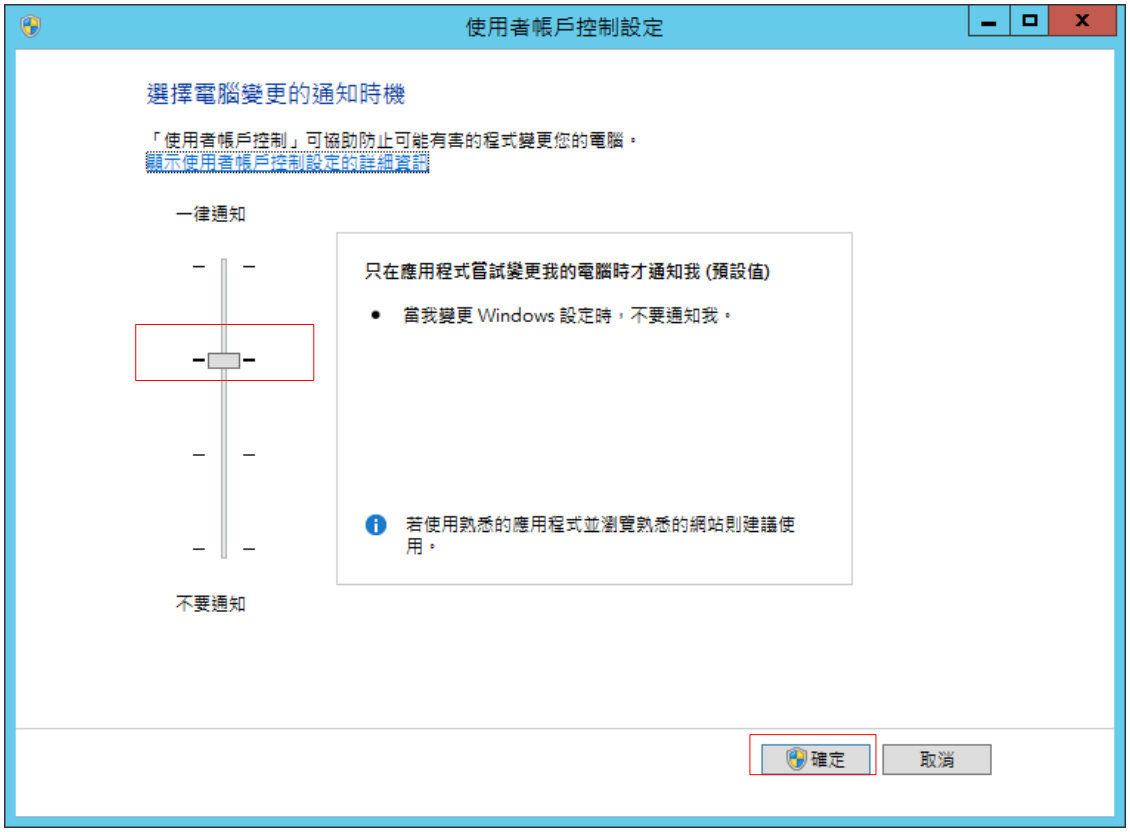
Step1 : 於電腦搜尋工具輸入-控制台

Step2 : 點擊[使用者帳戶]

Step3 : 再次[選取使用者帳戶]

Step4 : 開啟 UAC (使用帳戶控制)，選取[變更使用者帳戶控制設定]

Step 5 : 將左邊拉回初始值如下方紅框位置，再選取[確定]



Step 6 : 需重新啟動電腦，設定才會生效。

3.7 為什麼已開啟硬體驗證，仍會被要求輸入機碼?

- 可先檢查本機機碼，是否已加入至 Sever 的 TRS File Monitor 驗證清單列表中。
- 確認 TRS File Monitor 是否已安裝。
- 查看 TRS File Monitor 是否停止偵測，詳如 2.2 章節。
- Windows 遠端桌面連線(Remote Desktop Connection)的剪貼簿功能必須勾選，才能做 Client 端硬體驗證，詳如 3.14 章節。

3.8 Sever 已安裝 TRS File Monitor，本機未安裝，輸入亂數機碼時，為什麼會直接登出跳回本機?

- TRS File Monitor 為防止駭客攻擊，則將與機碼無關之按鍵鎖定，一旦使用者觸擊，則開

啟保護模式，直接從 Sever 登出。

- 使用者僅能使用: “Ctrl”、英文、數字、” - “ 等按鍵，除此以外則視為駭客攻擊。
- 按了 ALT 等鍵，嘗試離開驗證畫面。
- 為了防止駭客使用各種方式猜對亂數機碼，系統設定 30 秒內完成輸入，30 秒後未輸入完成，即登出。

3.9 Windows 工作列看不到 TRS File Monitor Icon?

- 使用者權限不足，安全性考量，系統管理者才能看到與使用。
- 因開機不須登入即已啟動保護，所以有時在控制台(Console Mode)模式下，系統管理者登出再取消登出，即能看到。

3.10 按 TRS File Monitor 的 Stop 可停止監測,是否也會停止防止勒索軟體功能?

在單人模式是:但在多人環境(Multi Session)下，仍舊保有防止勒索軟體功能。

3.11 按結束時或被強迫結束時,是否也會停止防止勒索軟體功能?

按結束時或被強迫結束時，會自動再被啟動，除非人工解除安裝(Uninstall)。

3.12 系統登出時,是否也會停止防止勒索軟體功能?

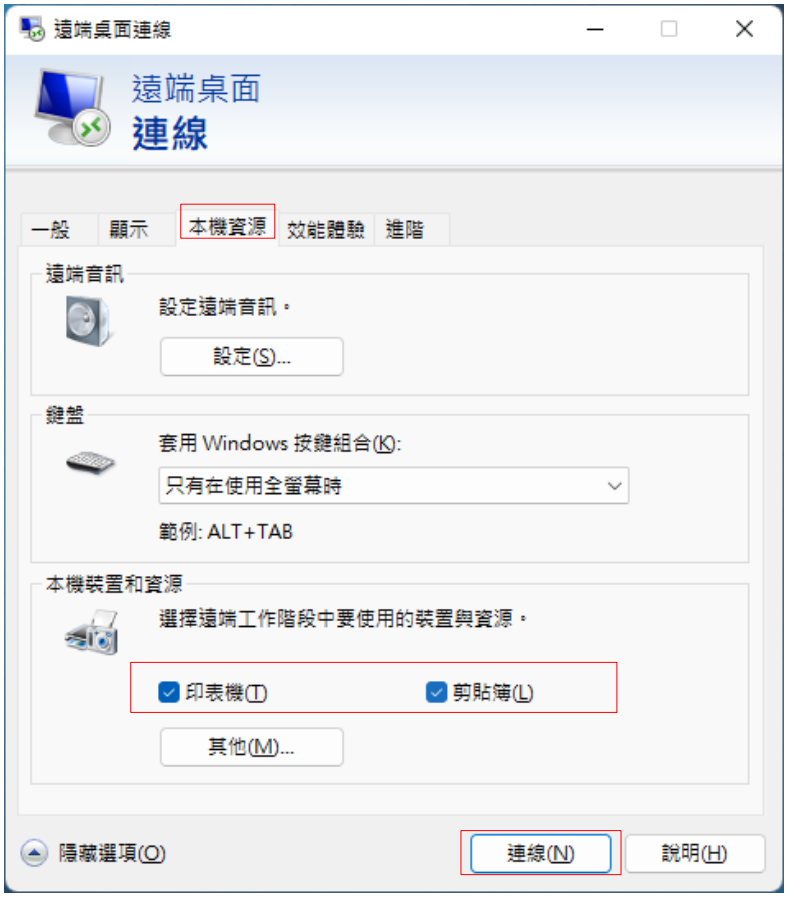
系統登出時，仍舊保有防止勒索軟體功能；在控制台(Console Mode)模式下，系統登出時會出現警示訊息，亦不會影響防止勒索軟體功能。

3.13 如何得知有偵測到可疑勒索軟體行為?

- 登入狀態下會出現下列警告訊息畫面，詳如 1.4 章節。
- 進入隔離區可看到依日期排序被隔離的程式，如程式重複被隔離僅會顯示第一次的日期，詳如 2.5 章節。
- 點擊 About 的 mail 圖示可看到可疑勒索軟體行為與隔離記錄，詳如 2.7.3 章節。

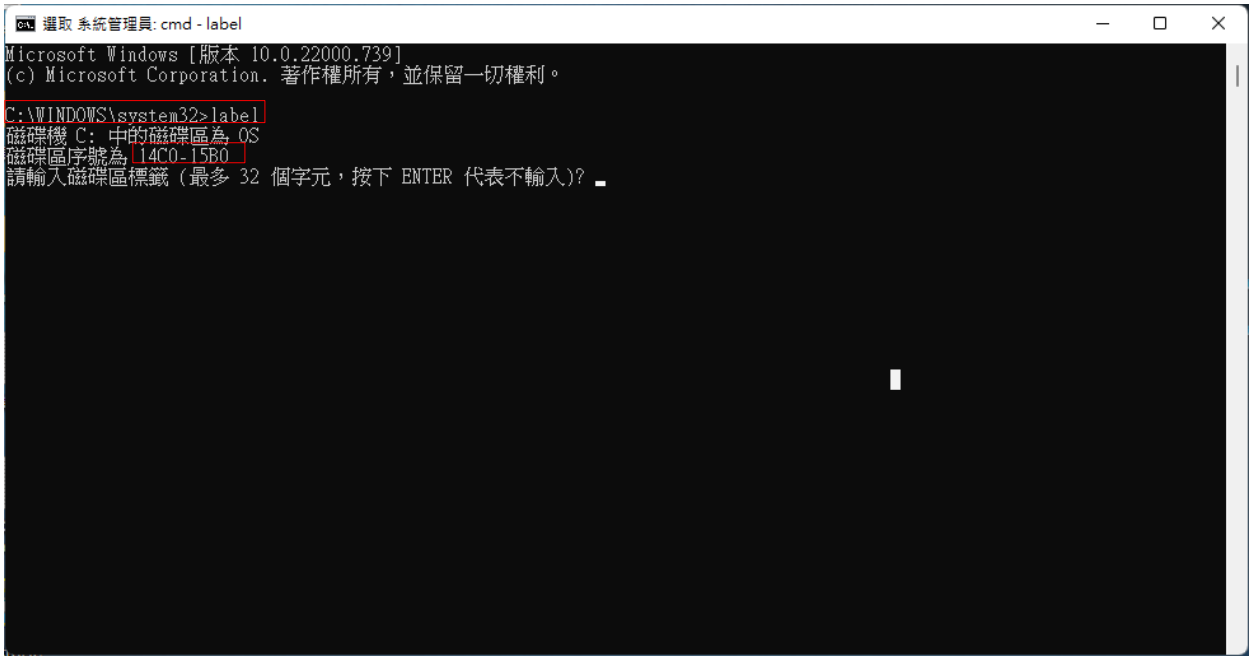
3.14 驗證(Verification)功能,是針對什麼做驗證?

- 專門針對 Windows 遠端桌面連線(Remote Desktop Connection)登入做 Client 端或 Server 端硬體驗證,防止使用者密碼被駭時，多一層更嚴密保護,讓行動辦公或遠端登入更安全，詳如 2.4 章節說明。
- Client 端若未安裝 TRS File Monitor ，例如用手機 RDC APP 登入，會自動做 Server 端硬體驗證。
- Client 端若有安裝 TRS File Monitor 時會自動驗證，不需輸入驗證碼，但驗證失敗時，亦會啟動 Server 端硬體驗證，可等 30 秒自動登出後再重新登入即可。
- Windows 遠端桌面連線(Remote Desktop Connection)的剪貼簿功能必須勾選，才能做 Client 端硬體驗證。如圖示

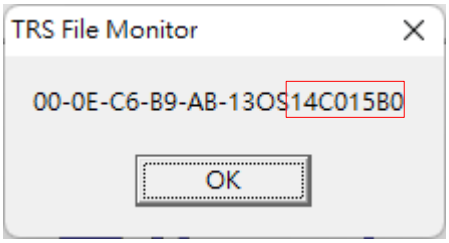


- Client 端或 Server 端硬體 TRS Verification Key 可隨時更改 Hard Disk C:磁碟的 Label 來變動 TRS Verification Key 的某一部份，以增加安全性。如圖示

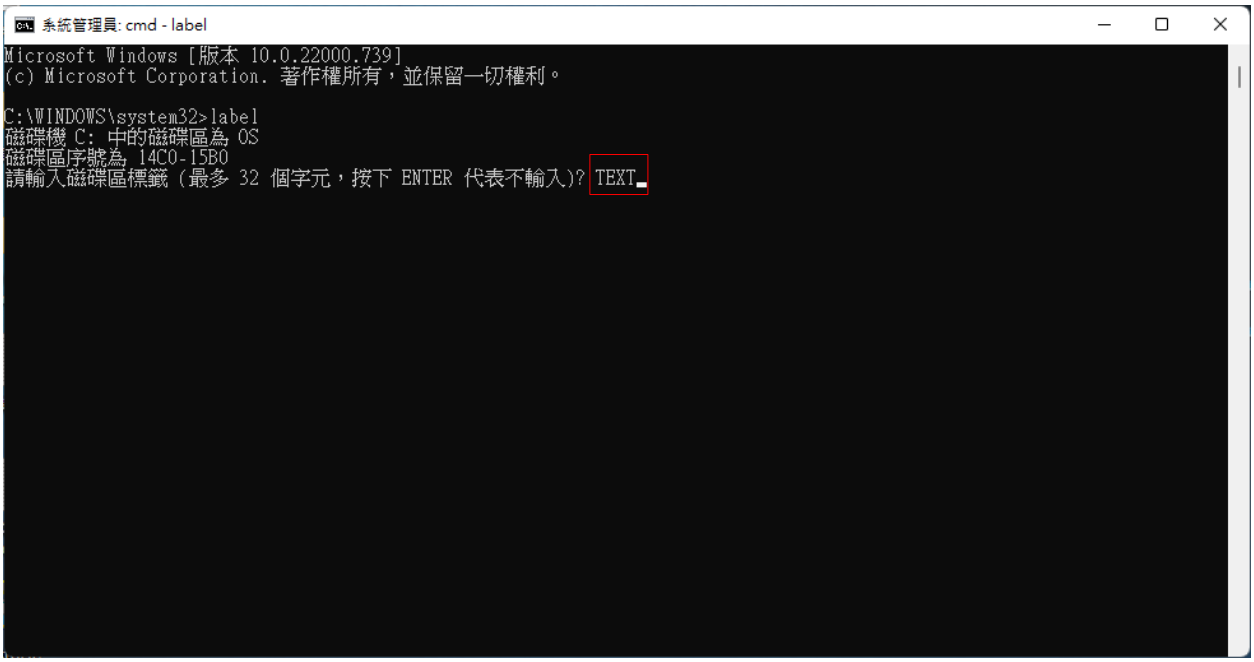
  Step1 : 更改前，使用系統管理員身分開啟 cmd 查詢當前 label 值，輸入: label



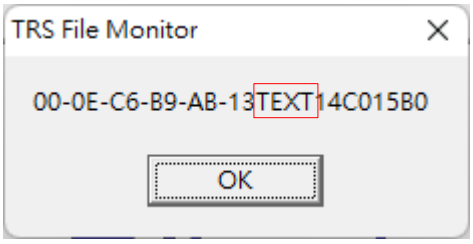
Step2 : 並以 2.4.1 章節方式開啟本機機碼



Step3 : 輸入欲更改之磁碟區名稱:TEXT (範例)

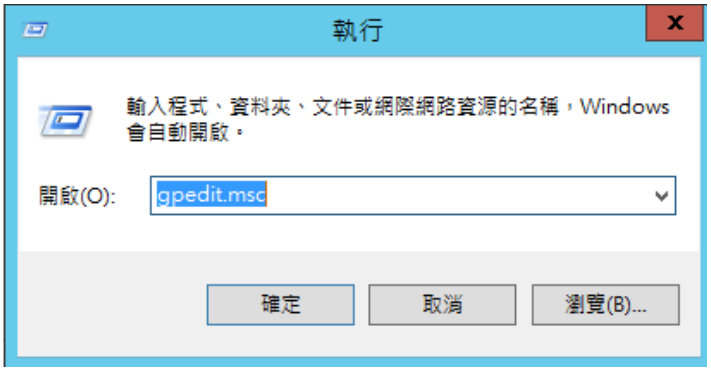


Step4 : 以 2.4.1 章節方式查詢更正後的機碼

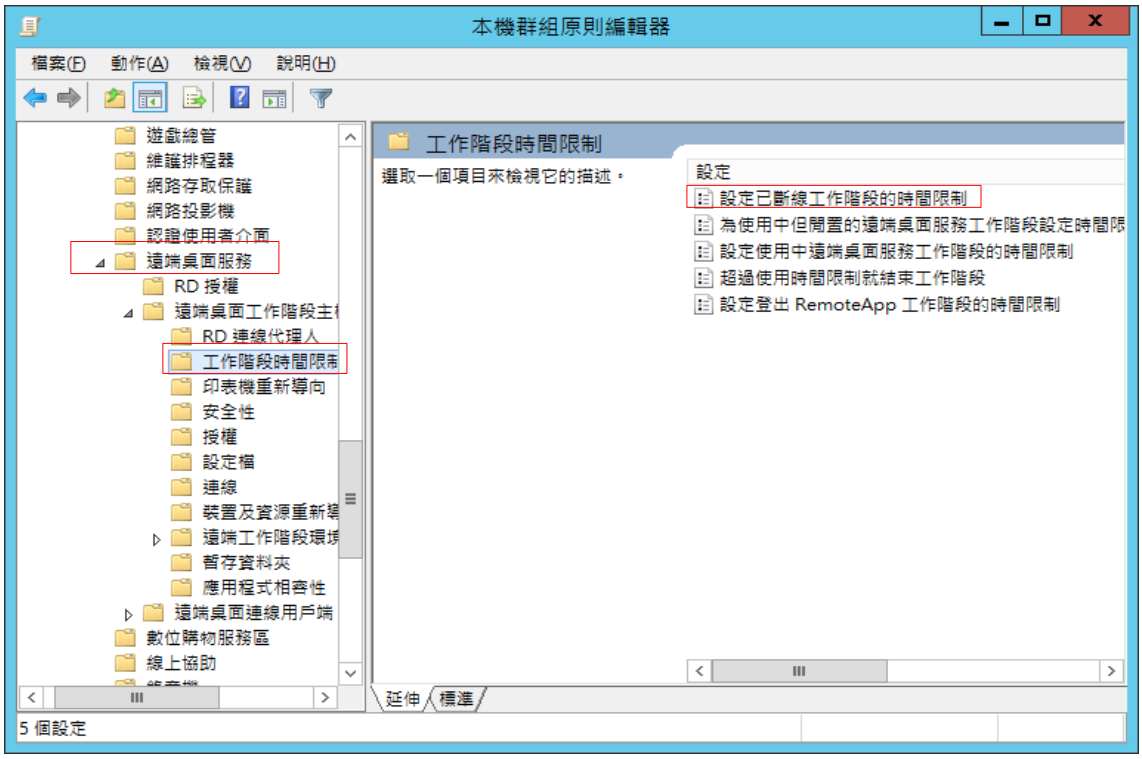


- Server 端啟動驗證功能時，若忘記 TRS Key 導致系統無法登入時，可由本機控制台進入，取得或設定 TRS Verification Key。詳 2.4.1 章節。
- RDC 斷線時必須設定即時登出，如圖示

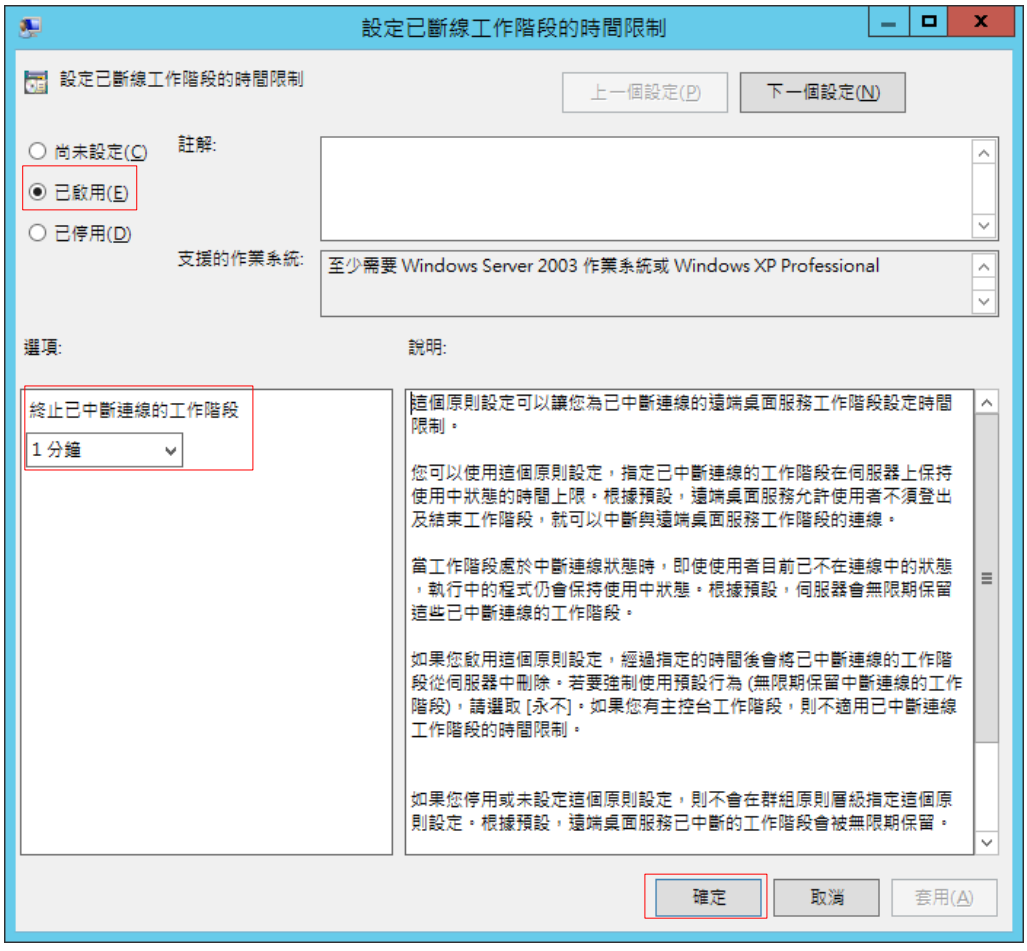
Step1 : 先開啟「群組物件原則編輯器」，輸入 gpedit.msc



Step2 : 找到 本機電腦原則 / 電腦設定 / 系統管理範本 / Windows 元件 / 遠端桌面服務(終端機服務) / 工作階段，選取”設定已斷線工作階段的時間限制”



Step3 : 設定已斷線工作階段的時間限制，勾選已啟用、設定分鐘數(依使用者狀況自行選擇)



- Servser 端硬體 TRS Verification Key 驗證碼須搭配動態值輸入，以增加安全性。

3.15 如何用複製(Ctrl+C)與剪貼(Ctrl+V)等功能, 輸入 Server 端驗證碼?

必須在出現 Server 端驗證畫面時，切換至 Client 端,複製(Ctrl+C)字串，再切換至 Server 端驗證畫面，在驗證欄位剪貼(Ctrl+V)字串。

3.16 為何遠端桌面連線(Remote Desktop Connection)的剪貼功能無效?

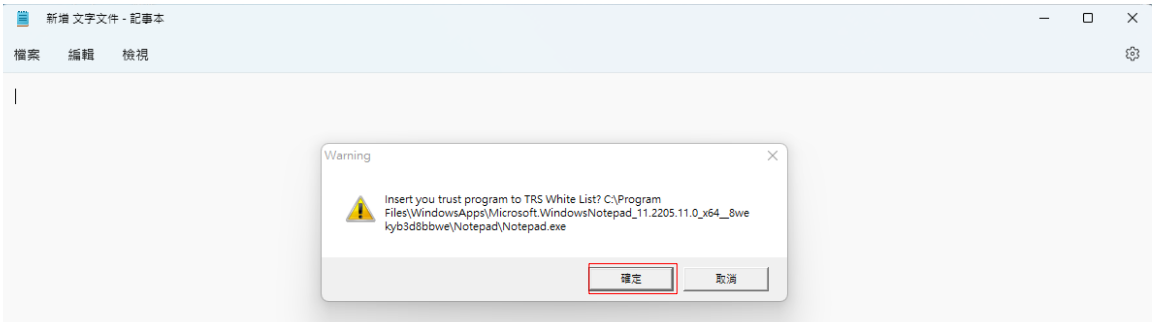
啟用驗證(Verification)功能時，必須登入驗證後，剪貼功能才能正常使用。

3.17 開啟合法程式時被誤判為勒索軟體, 出現警告訊息, 程式無法正常使用?

可至隔離區(Isolation)將該程式恢復(Restore)即可正常使用，詳如 2.5 章節。

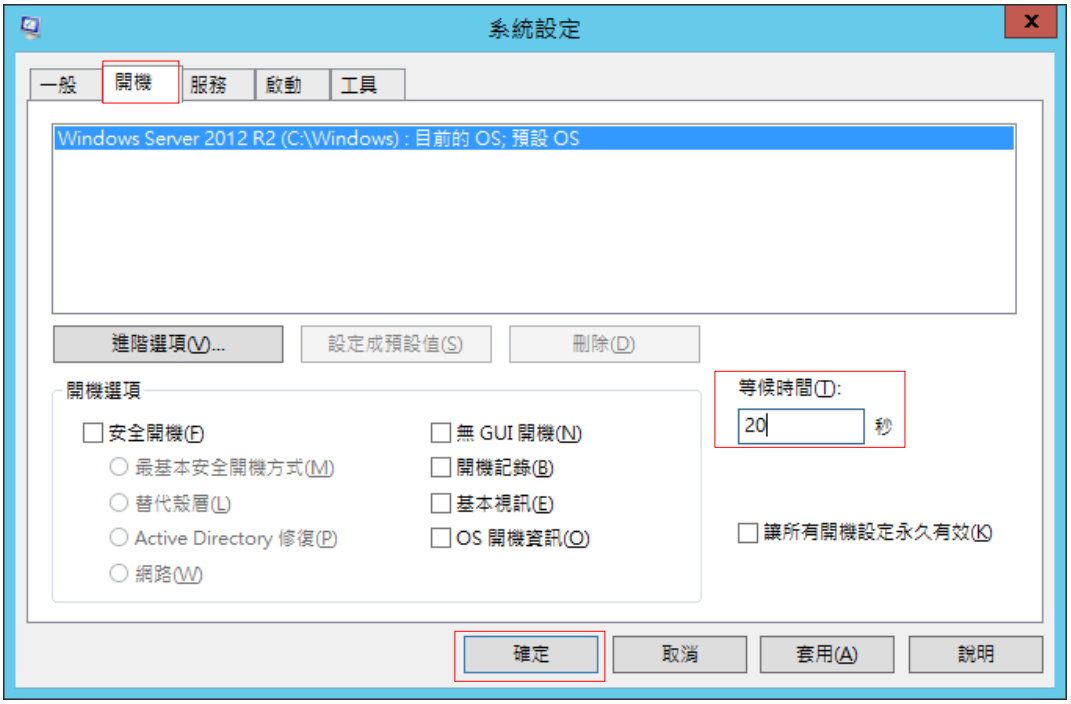
3.18 突然出現是否將程式加入白名單的訊息,是否該加入?

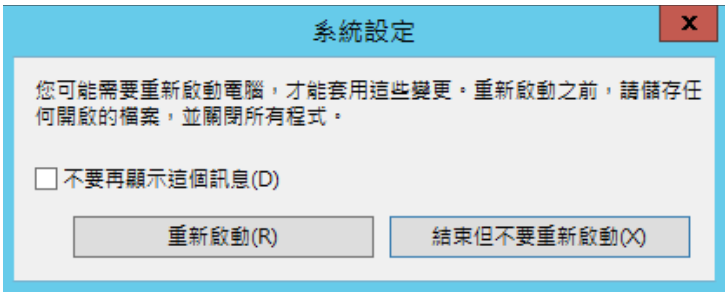
如果訊息是由人工開啟程式過程中即時出現的，例如使用者開啟記事本時，出現此訊息，可安心加入記事本於白名單，以避免程式在執行過程中被強迫結束，如圖示

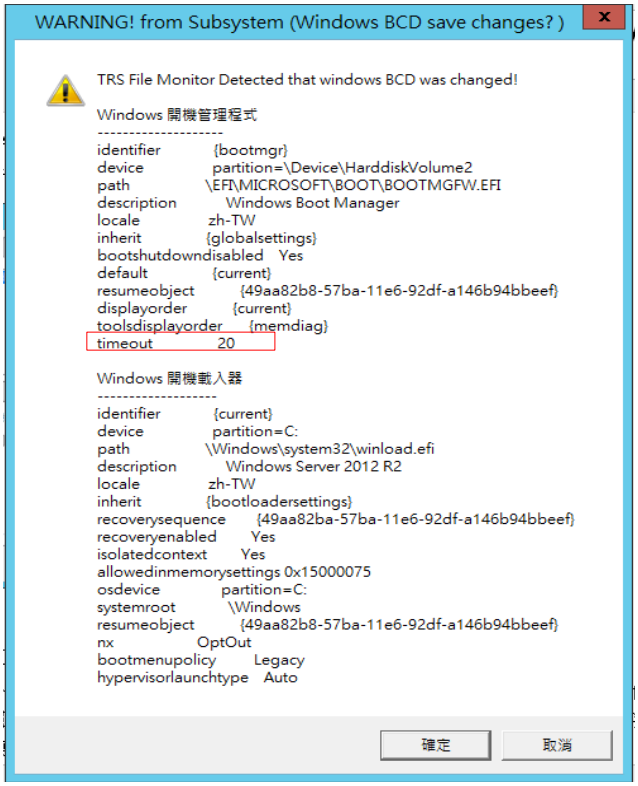


3.19 執行 Msconfig.exe 修改開機資料無效?

因未對下列訊息做確認，如圖示







3.20 使用 TRS File Monitor 是否有個資外洩的風險?

不同於其他軟體會將使用者電腦各種資訊傳回，TRS File Monitor 不連線外部任何主機，徹底杜絕個資外洩的風險（縱然是經由使用者允許，寄回可疑勒索行為記錄協助判讀時亦然），遵循歐盟防止個資外洩的規範。

3.21 如何建構一個防止勒索軟體的環境

- 良好的備份與還原(即時/批次/異地)
  依可接受的風險，做合理的設備投資。
- 落實資安政策管理(windows 設定/權限管理/防火牆管理)
  1. windows 設定:啟動 UAC(User Account Control)等。
  2. 權限管理:儘量不以系統管理者權限登入。
  3. 防火牆:定期檢視硬體與軟體防火牆，管制 DNS 與 IP 及 Port 等。
- 安裝 TRS File Monitor-Anti Ransomware
  能對防火牆(port 135/139/445)，PSEXEC、PowerShell、BCD(Boot Config Database)、API Hook、遠端桌面連線(Remote Desktop Connection)、DOS Command(Regedit、WMIC…)及可疑勒索行為等，做有效防護。