



資訊處
Office of Information Technology

個人電腦安全設定手冊

Windows 10版



一、Windows Update、防火牆及校時等設定

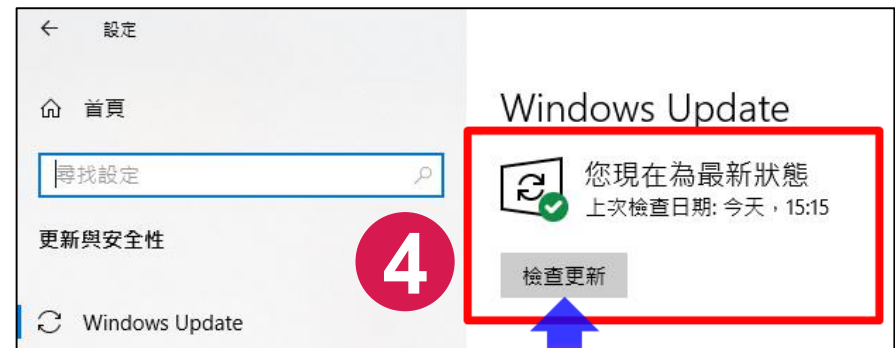
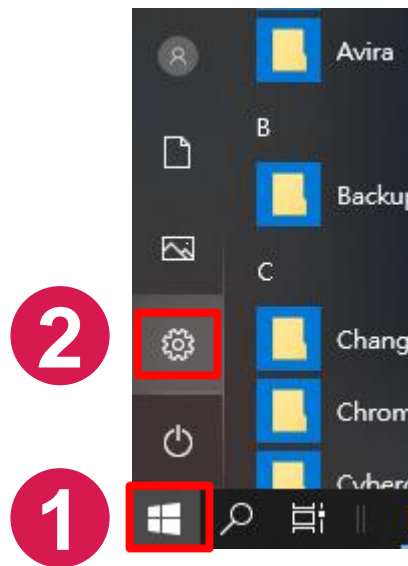


使用者電腦安全設定

- 一、Windows update更至最新版
- 二、啟用防火牆
- 三、關閉遠端登入 (RDP)
- 四、設定校時
- 五、取消使用者帳號密碼永久有效

一、使用Win10 (Windows update至最新版)

- 一、下載安裝Windows 10：請至校園軟體下載 <https://software.ccu.edu.tw/>
- 二、點選左下角Windows圖像→點選【設定】→選擇【更新與安全性】
- 三、檢查更新：確認為最新狀態，如果不是請依系統指示進行更新（**很重要**）
- 四、如果無法完全更新請先移除防毒軟體，更新完後再安裝防毒軟體。
- 五、點選左下角Windows圖像，按**右鍵**點選【系統】→【關於】拉到下方有版本及日期，因主機不同有不同版本（最新**22H2**版，若是**21H2**以前版本請確認是否可以更新）



可能要重新開關機多次才能完全更新（**很重要**）

二、啟用防火牆 1/2

- 一、點選左下角Windows圖像→點選【設定】 →選擇【更新與安全性】
- 二、在左側欄點選【Windows安全性】，右側欄點選【防火牆與網路防護】
- 三、逐一確認【網域網路】、【私人網路】及【公用網路】防火牆是否開啟



The image shows two side-by-side screenshots of the '防火牆與網路保護' (Firewall & Network Protection) settings page. The left screenshot shows the 'Windows Defender Firewall' status as '已開啟' (On) for all three network types: '網域網路' (Domain network), '私人網路' (Private network), and '公用網路' (Public network). The right screenshot shows the 'Other Windows Firewall' status as '已開啟' (On) for all three network types. Red boxes and numbers 3, 4, and 5 highlight the status of each network type in both screenshots.

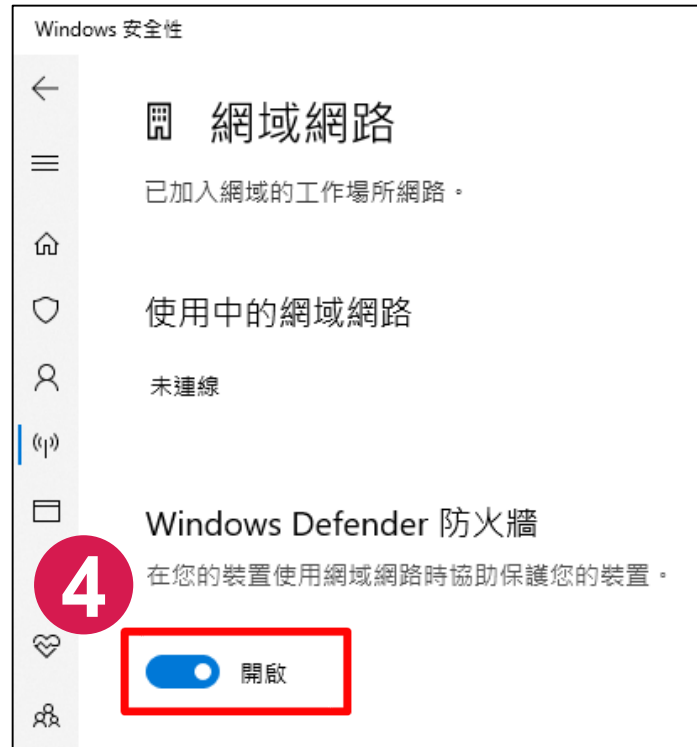
已開啟Windows Defender防火牆

已開啟其他防火牆

已設定防火牆如圖例，不符合者下頁接續設定

二、啟用防火牆 2/2

四、如尚未開啟，逐一點選進入各(網域/私人/公用)網路設定，開啟 Windows Defender 防火牆



開啟 Windows Defender 防火牆



開啟防毒軟體防火牆
以 Trend Apex One 為例

三、關閉遠端登入 (RDP)

一、點選左下角Windows圖像，點選【設定】→【系統】，在左側欄點選【遠端桌面】（要捲到下面才看的到）

二、將啟用遠端桌面設為【關閉】

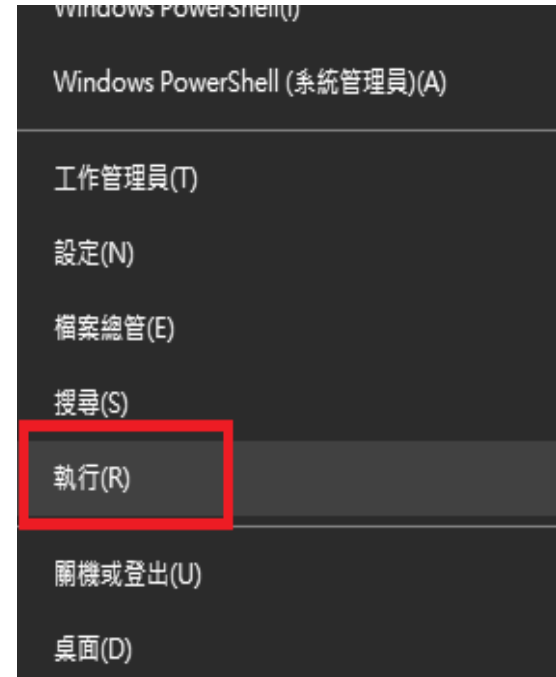


四、設定校時 1/3

一、按住鍵盤上Windows圖標鍵+R 在執行對話方塊，輸入【control】



鍵盤上Windows圖標鍵+R



參考：如果鍵盤上沒有Windows圖標鍵，請在左下角Windows圖示按滑鼠右鍵選「執行」，輸入【control】

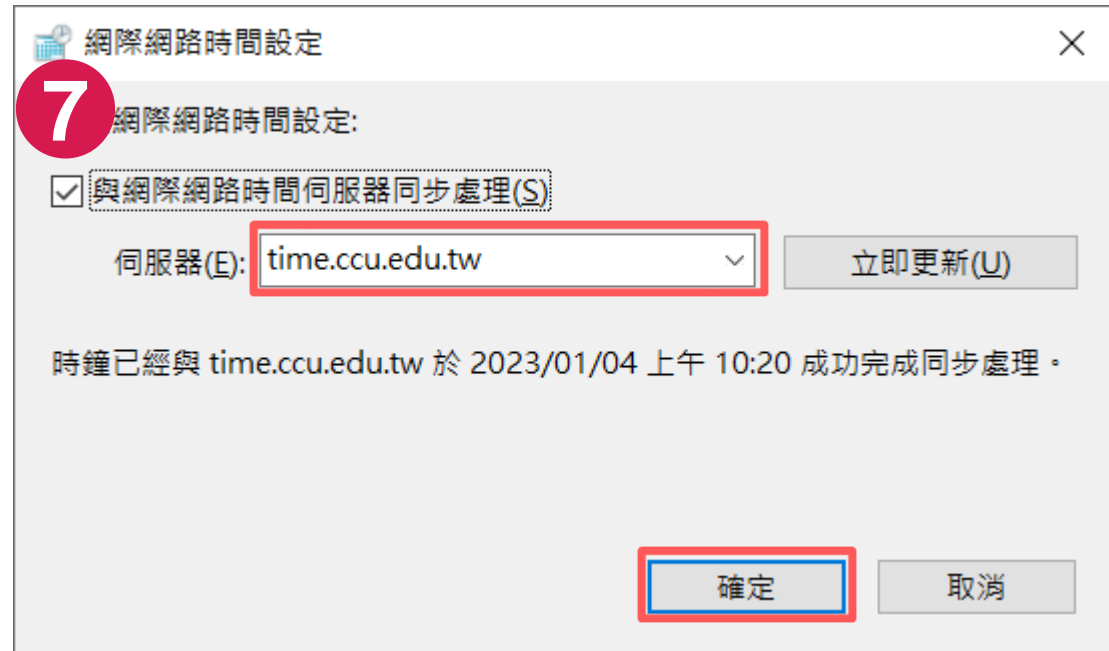
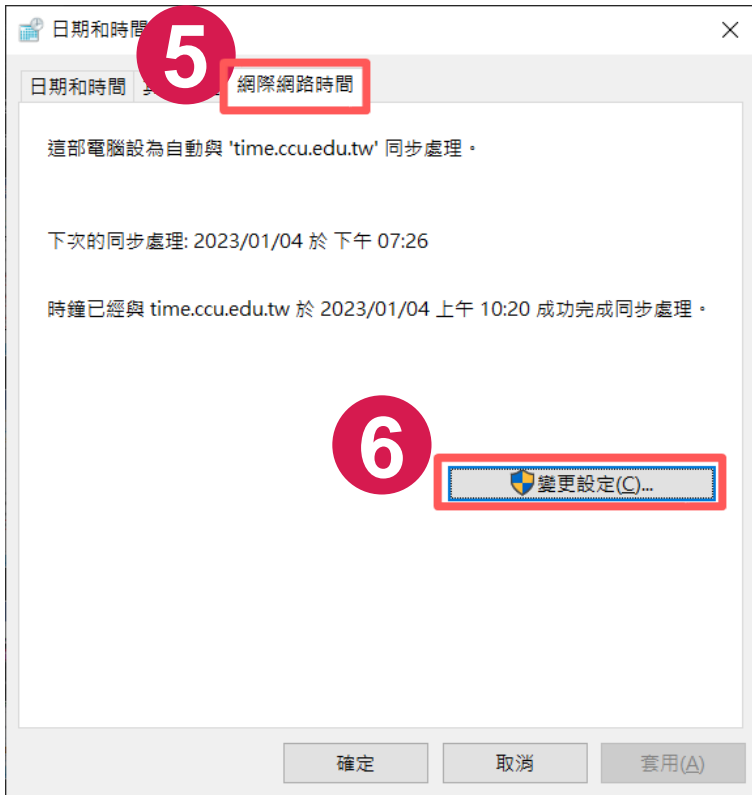
四、設定校時 2/3

二、依序點選【時鐘和區域】→【設定時間和日期】



四、設定校時 3/3

三、點選【網際網路時間】→【變更設定】，修改後點選確定



請設定本校校時伺服器：time.ccu.edu.tw

五、取消使用者帳號密碼永久有效 1/2

- 一、按住鍵盤上Windows圖標鍵+E 啟動檔案總管，於本機圖示點擊滑鼠右鍵叫出選單，點選【管理】

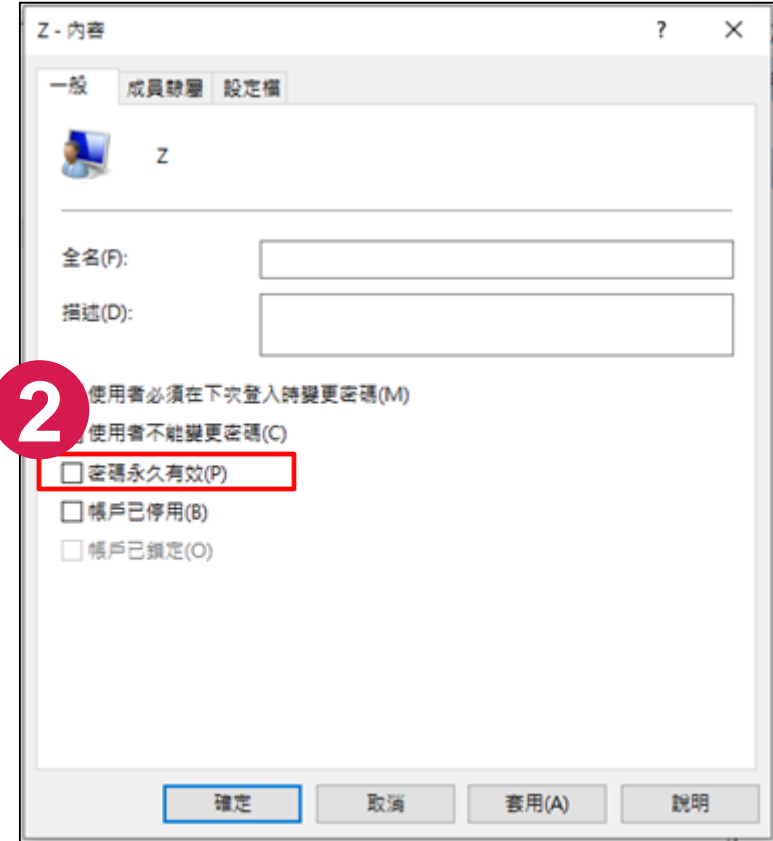
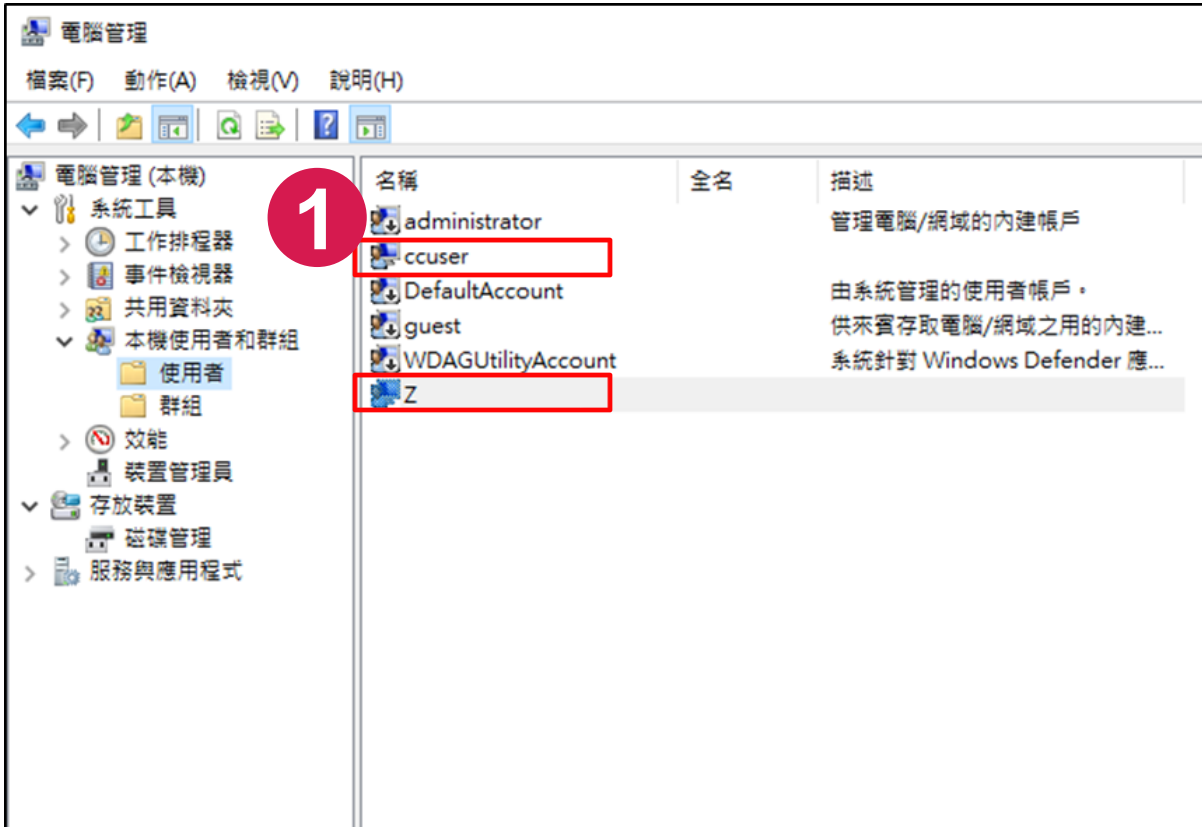


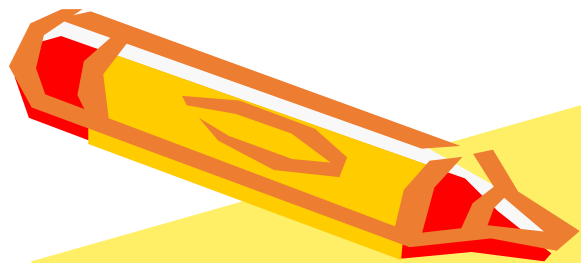
鍵盤上Windows圖標鍵+E



五、取消使用者帳號密碼永久有效 2/2

二、電腦管理-本機使用者與群組-使用者，逐一點選未停用的使用者帳號，確認未勾選「密碼永久有效」





二、本機安全性相關設定 (已安裝VANS agent者免設定)



本機安全性相關設定

➤ 需檢查**13項WINDOWS 10**安全性相關設定。

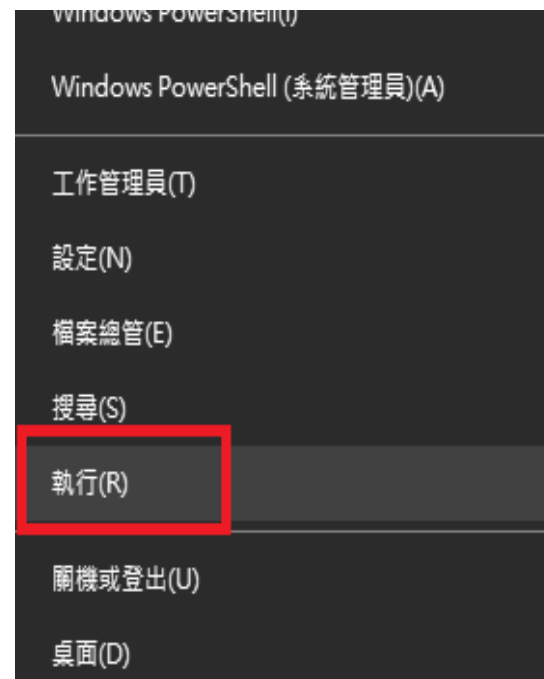
項次	安全性設定名稱	GCB設定值
1	密碼必須符合複雜性需求	啟用(英數字需混用)
2	密碼最長使用期限	90天
3	密碼最短使用期限	1 天
4	強制執行密碼歷程記錄	3以上記憶的密碼
5	最小密碼長度	8個字元以上
6	帳戶鎖定閾值	5次不正確的登入嘗試
7	重設帳戶鎖定計數器的時間	15分鐘
8	帳戶鎖定期間	15分鐘
9	帳戶：Guest 帳戶狀態	停用
10	關機：允許不登入就將系統關機	啟用
11	啟用螢幕保護裝置	啟用
12	以密碼保護螢幕保護裝置	啟用
13	螢幕保護裝置逾時	啟用，600秒

一、本機安全性原則

步驟一：按住鍵盤上Windows圖標鍵+R 在執行對話方塊，輸入 **【secpol.msc】**



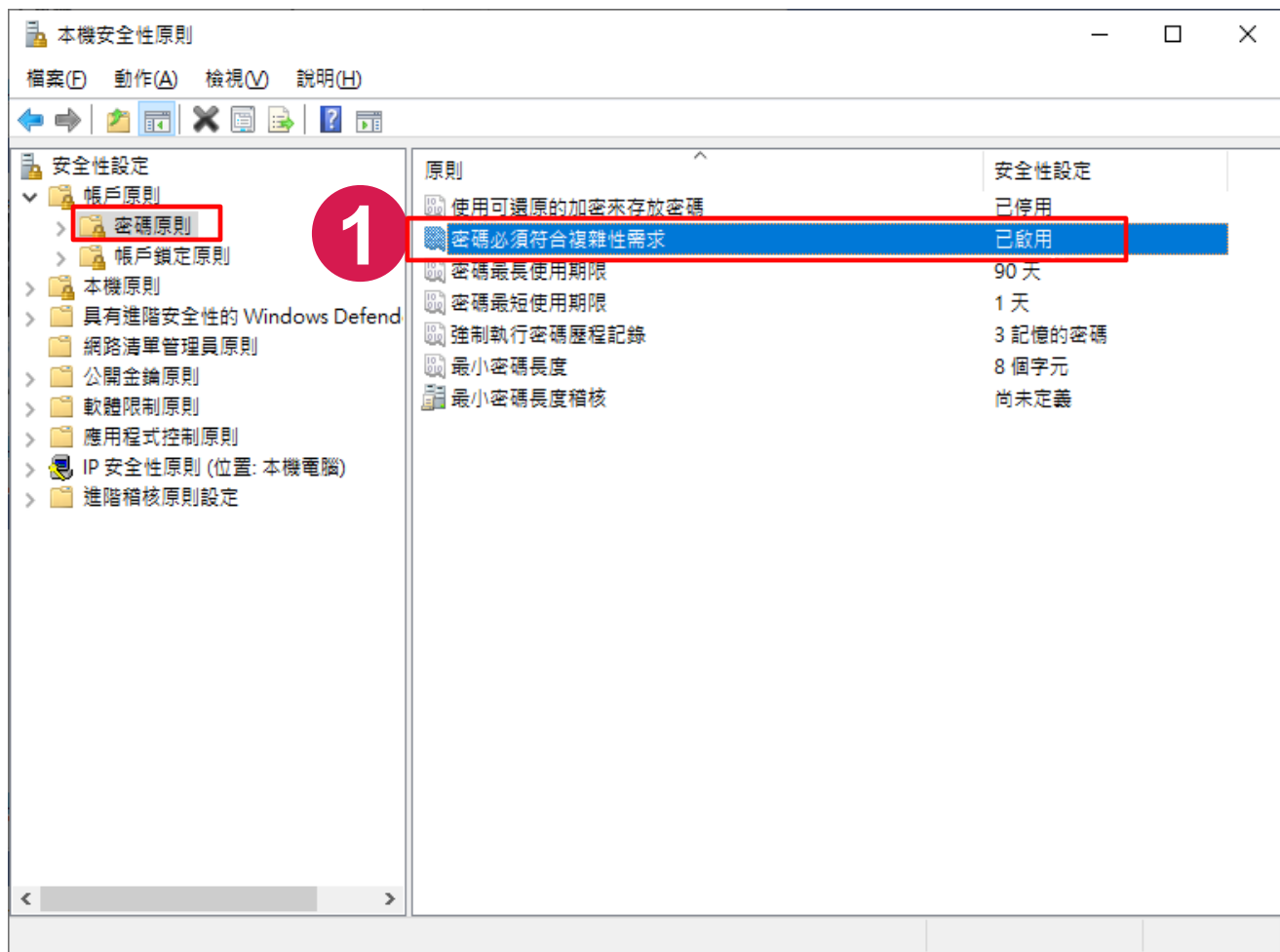
鍵盤上Windows圖標鍵+R



參考：如果鍵盤上沒有Windows圖標鍵，請在左下角Windows圖示按滑鼠右鍵選「執行」，輸入 **【secpol.msc】**

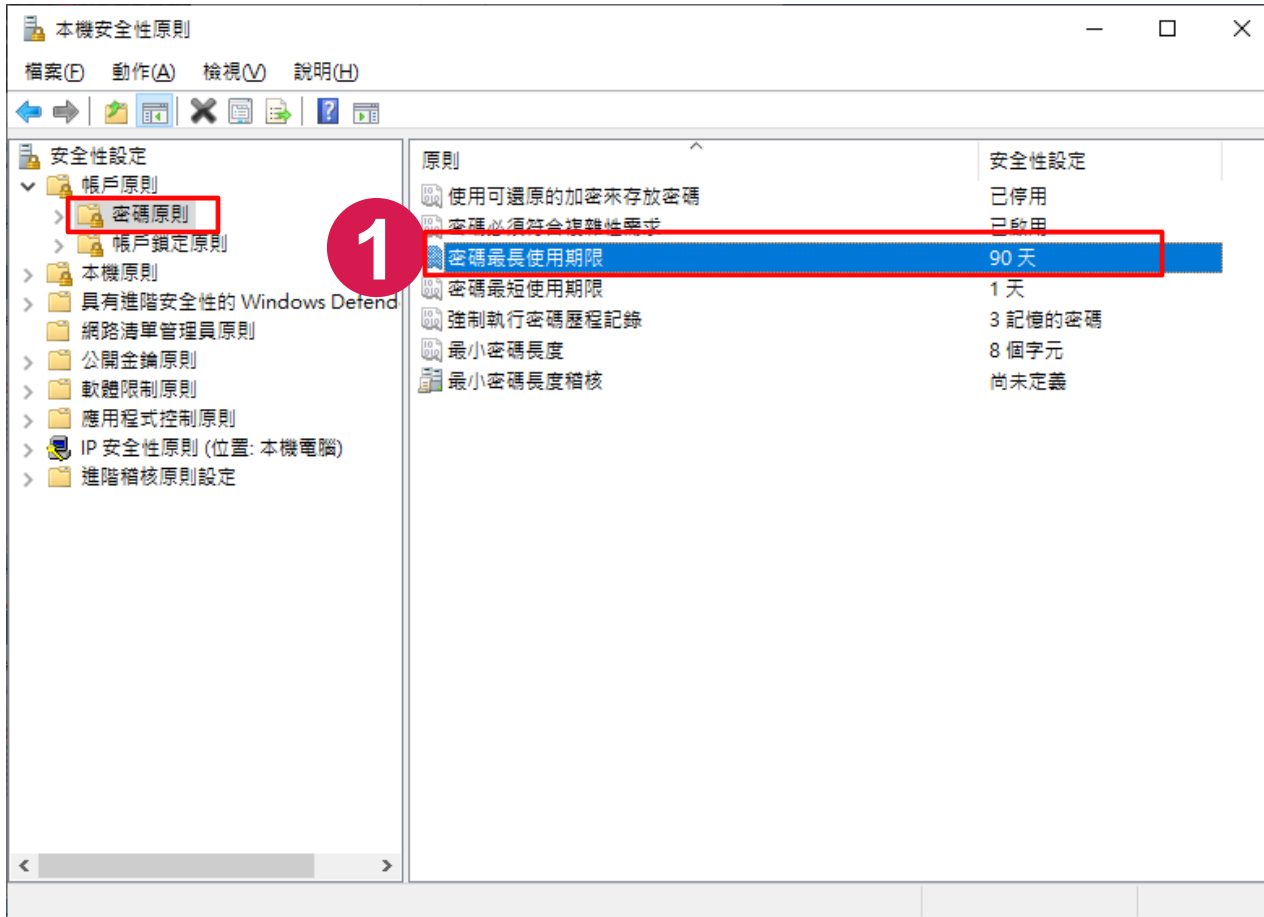
1. 密碼必須符合複雜性需求

1. 安全性設定-密碼原則-密碼必須符合複雜性需求-已啟用



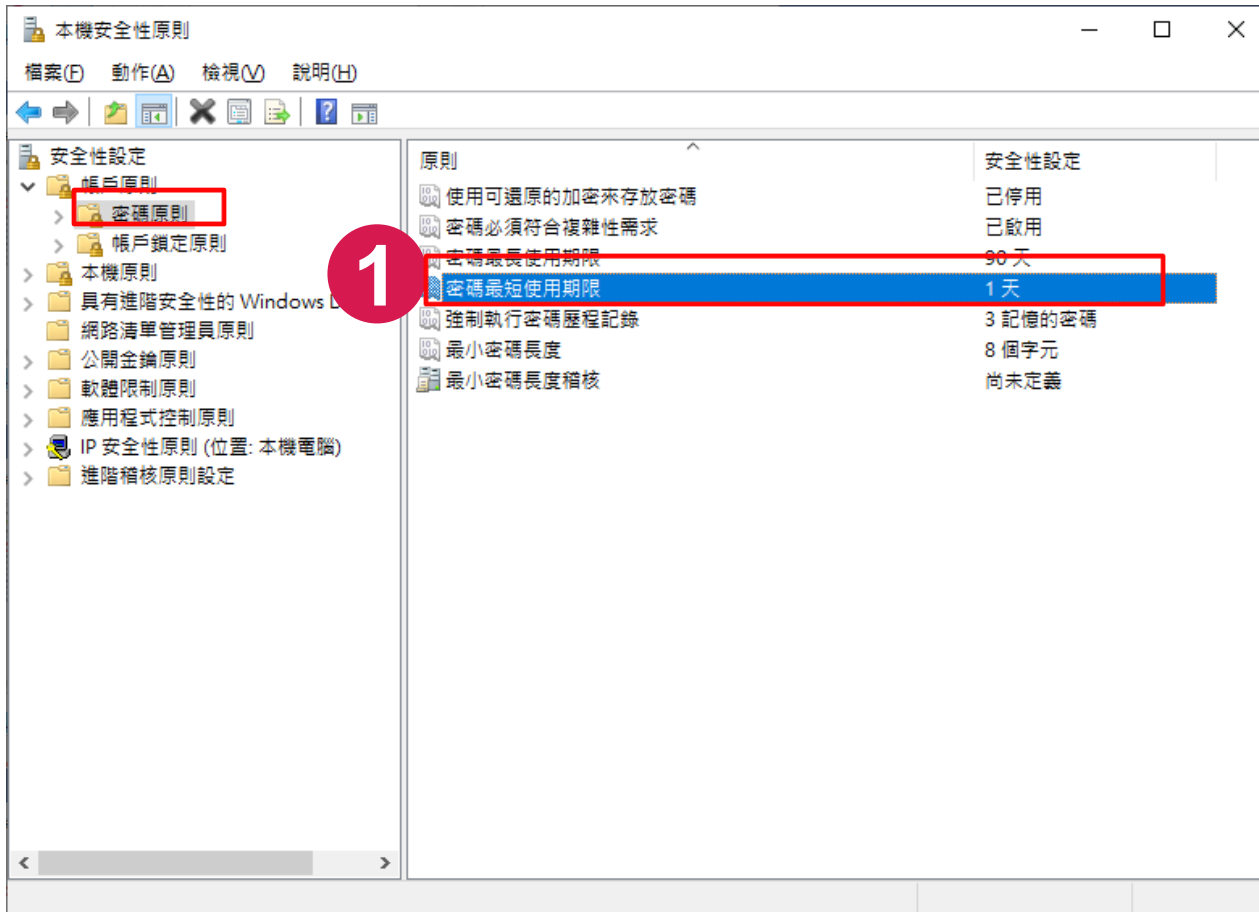
2. 密碼最長使用期限

2. 安全性設定-密碼原則-密碼最長使用期限-90天



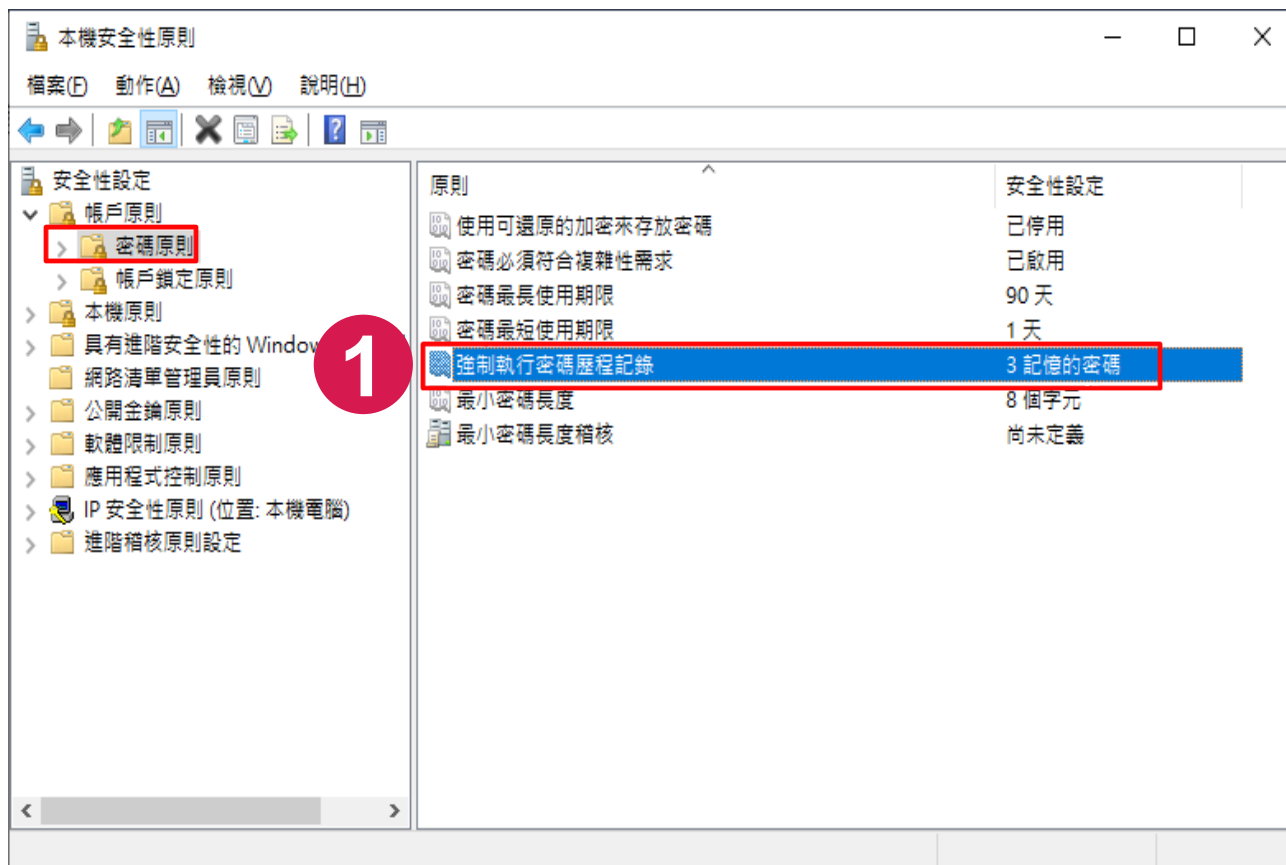
3. 密碼最短使用期限

3. 安全性設定-密碼原則-密碼最短使用期限-1天



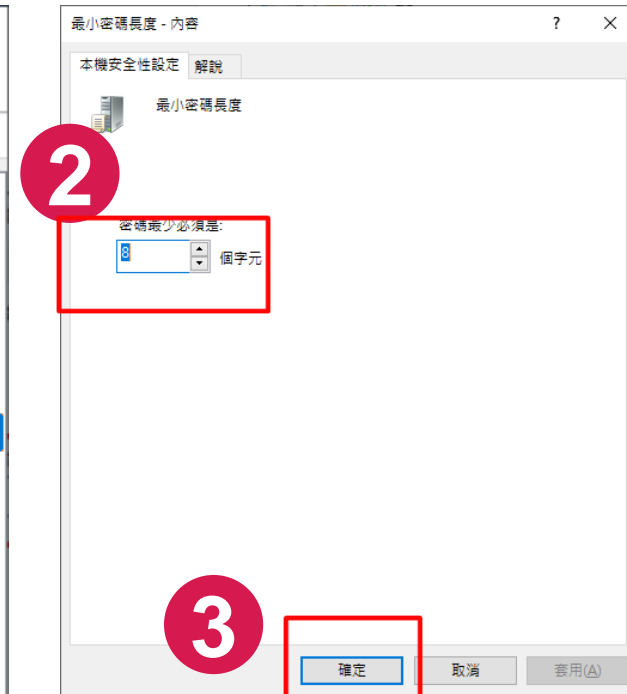
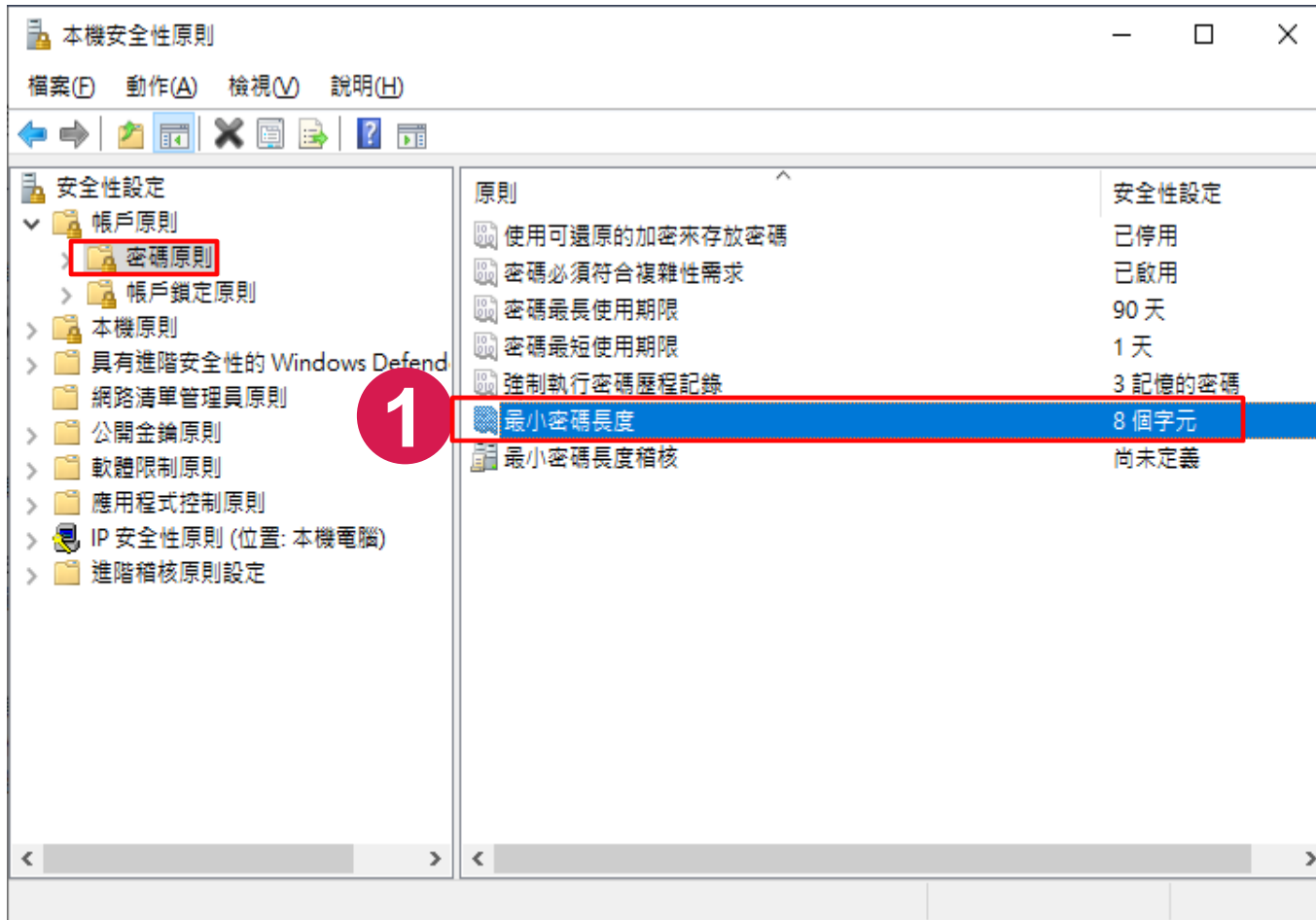
4. 強制執行密碼歷程紀錄

4. 安全性設定-密碼原則-強制執行密碼歷程紀錄-3次



5. 最小密碼長度

5. 安全性設定-密碼原則-最小密碼長度-8個字元以上



6~8. 帳戶鎖定原則

6. 安全性設定-帳戶鎖定原則-帳戶鎖定閾值-5次（注意順序不可以錯！）
7. 安全性設定-帳戶鎖定原則-重設帳戶鎖定計數器的時間間隔碼長度-15分鐘
8. 安全性設定-帳戶鎖定原則-帳戶鎖定時間-15分鐘

本機安全性原則

檔案(F) 動作(A) 檢視(V) 說明(H)

安全性設定

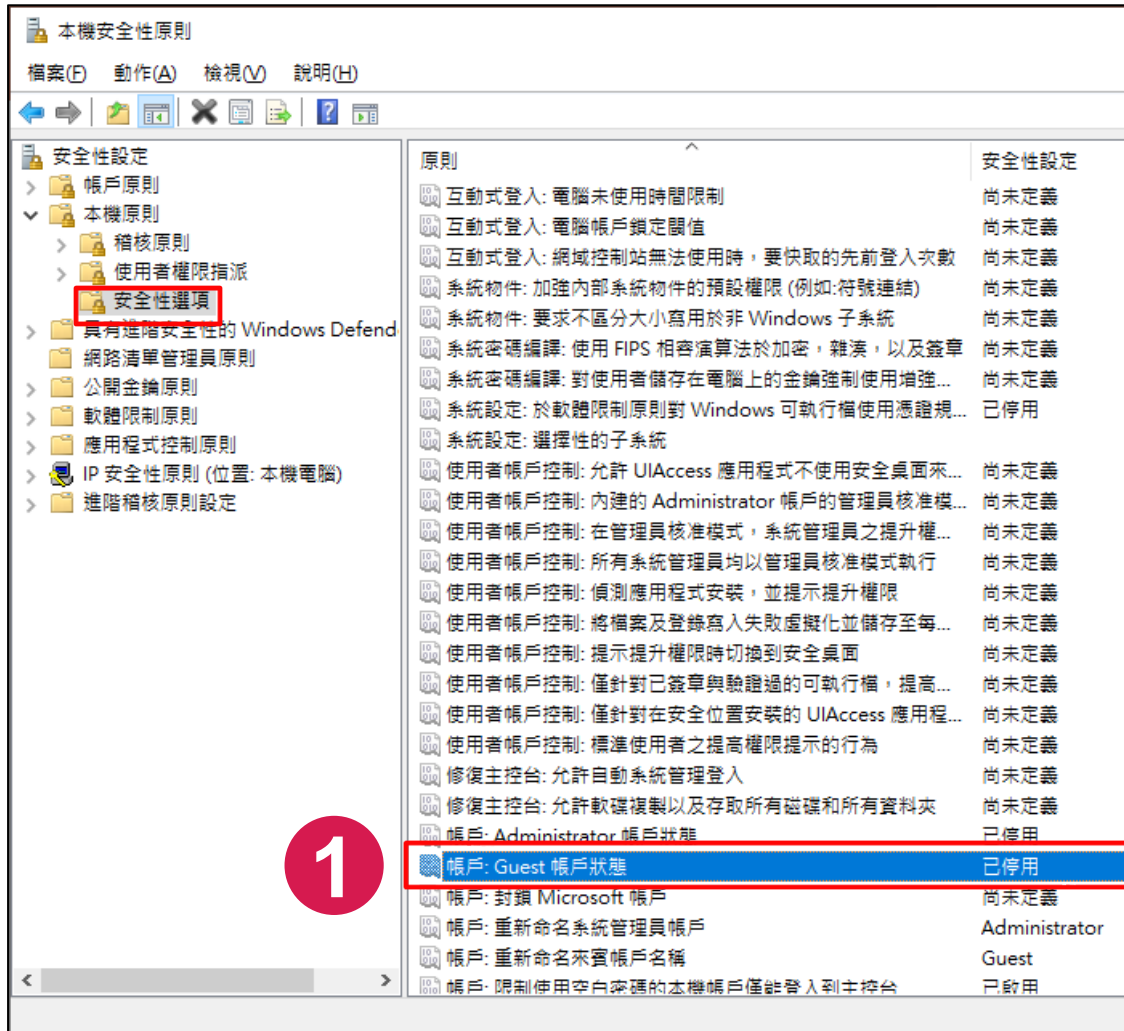
- 帳戶原則
 - 密碼原則
 - 帳戶鎖定原則
- 本機原則
- 具有進階安全性的 Windows Defender
- 網路清單管理員原則
- 公開金鑰原則
- 軟體限制原則
- 應用程式控制原則
- IP 安全性原則 (位置: 本機電腦)
- 進階稽核原則設定

原則	安全性設定
重設帳戶鎖定計數器的時間間隔	15 分鐘
帳戶鎖定時間	15 分鐘
帳戶鎖定閾值	5 次不正確的登入嘗試

注意：順序不可以錯！先設定帳戶鎖定閾值

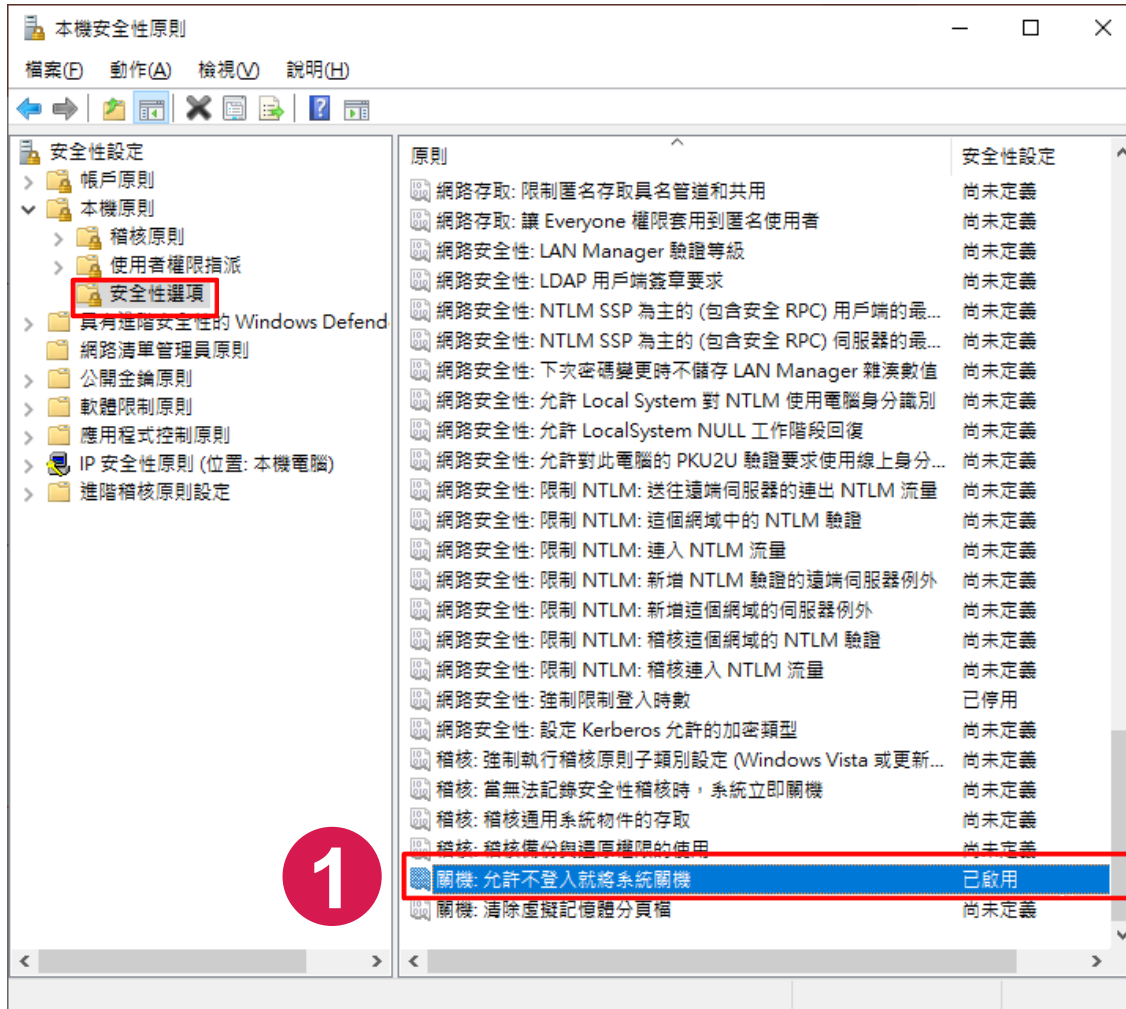
9. 帳戶：Guest 帳戶狀態

9. 安全性設定-本機原則-安全性選項-帳戶：Guest 帳戶狀態-已停用



10. 關機：允許不登入就將系統關機

10. 安全性設定-本機原則-安全性選項-關機：允許不登入就將系統關機-已啟用

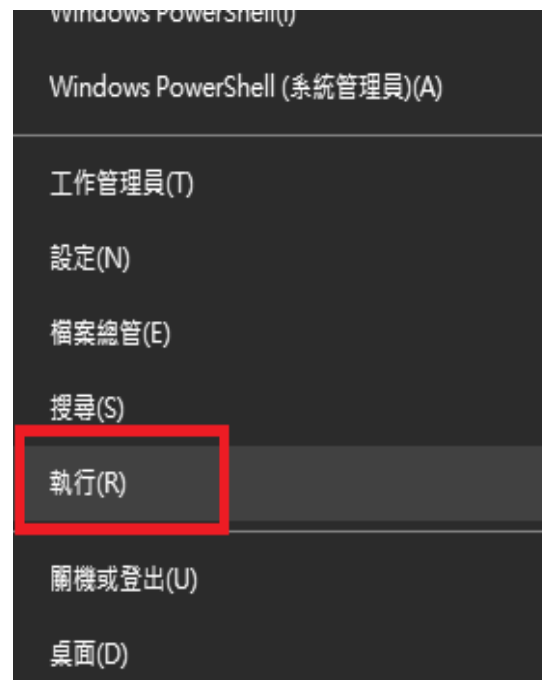


二、本機群組原則編輯器

步驟一：按住鍵盤上Windows圖標鍵+R 在執行對話方塊，輸入【gpedit.msc】



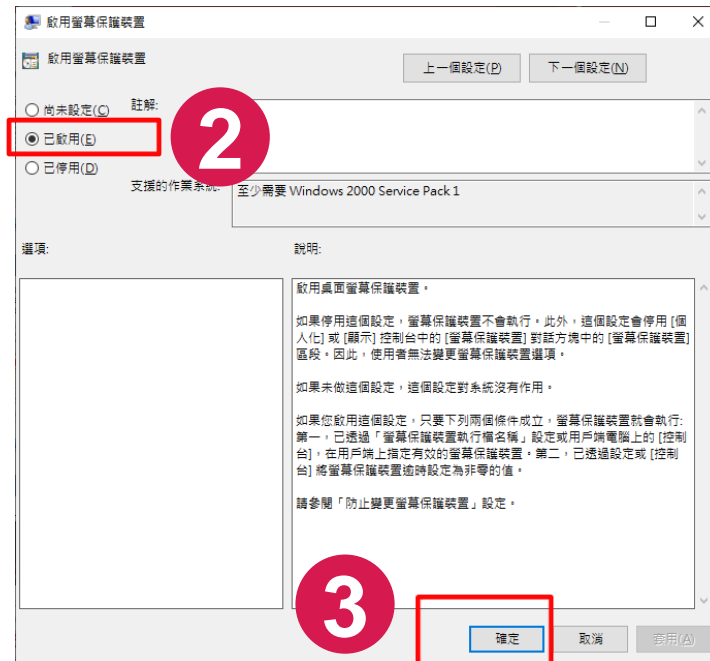
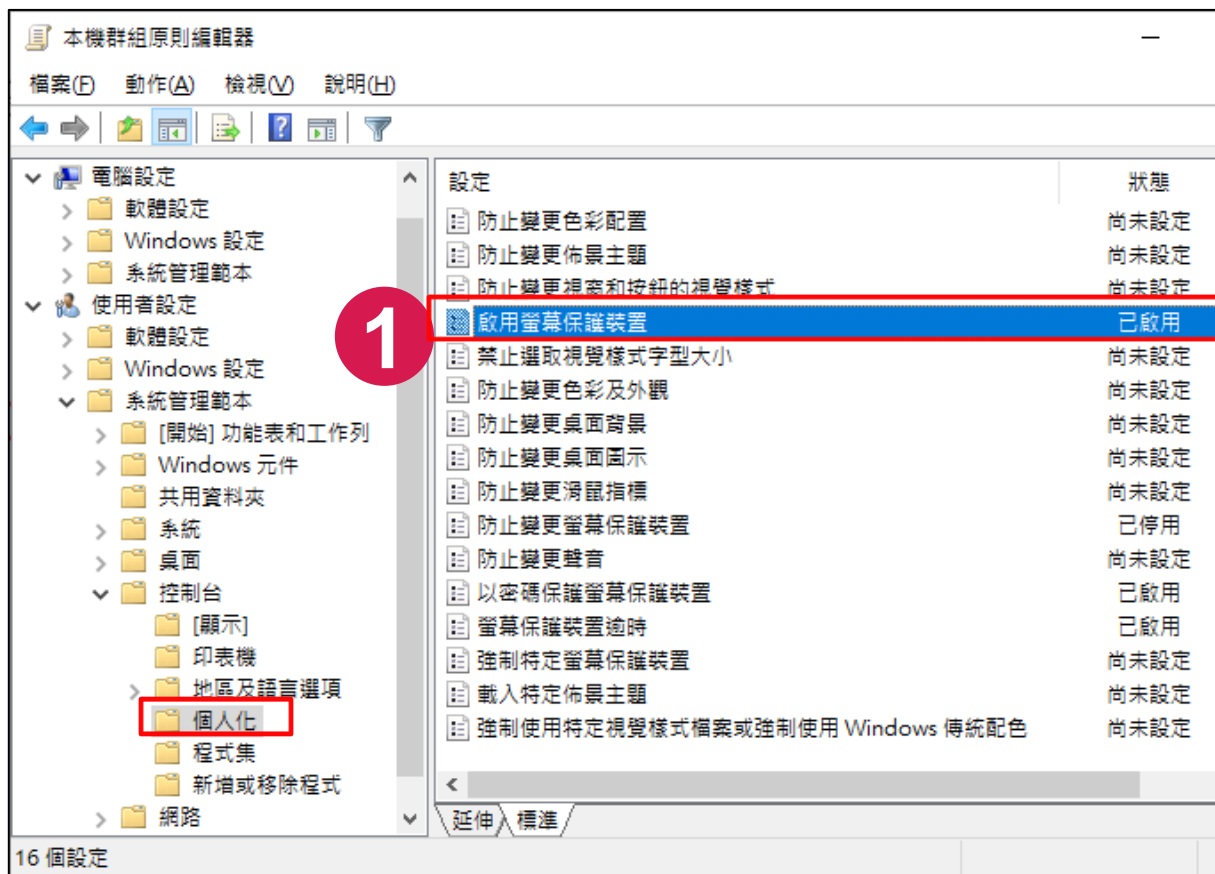
鍵盤上Windows圖標鍵+R



參考：如果鍵盤上沒有Windows圖標鍵，請在左下角Windows圖示按滑鼠右鍵選「執行」，輸入【gpedit.msc】

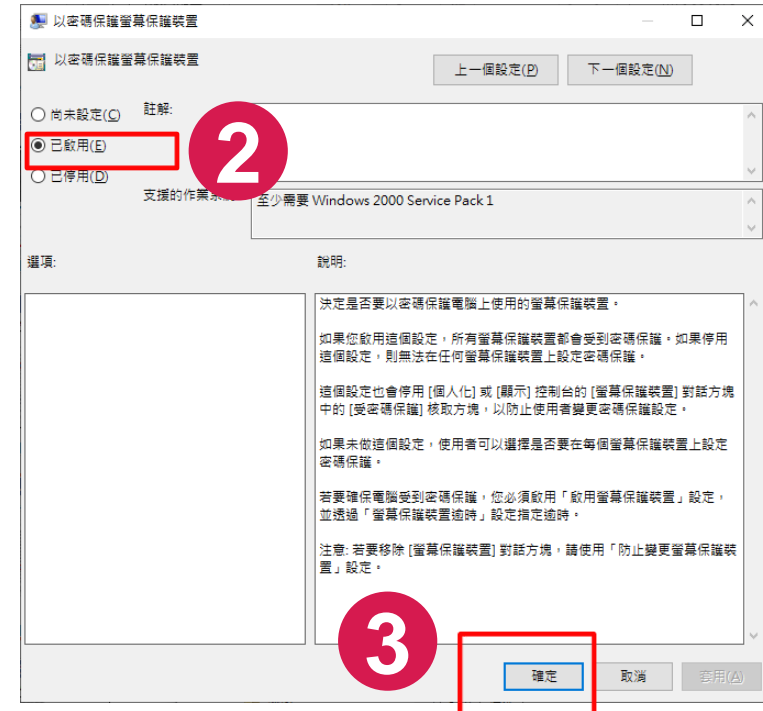
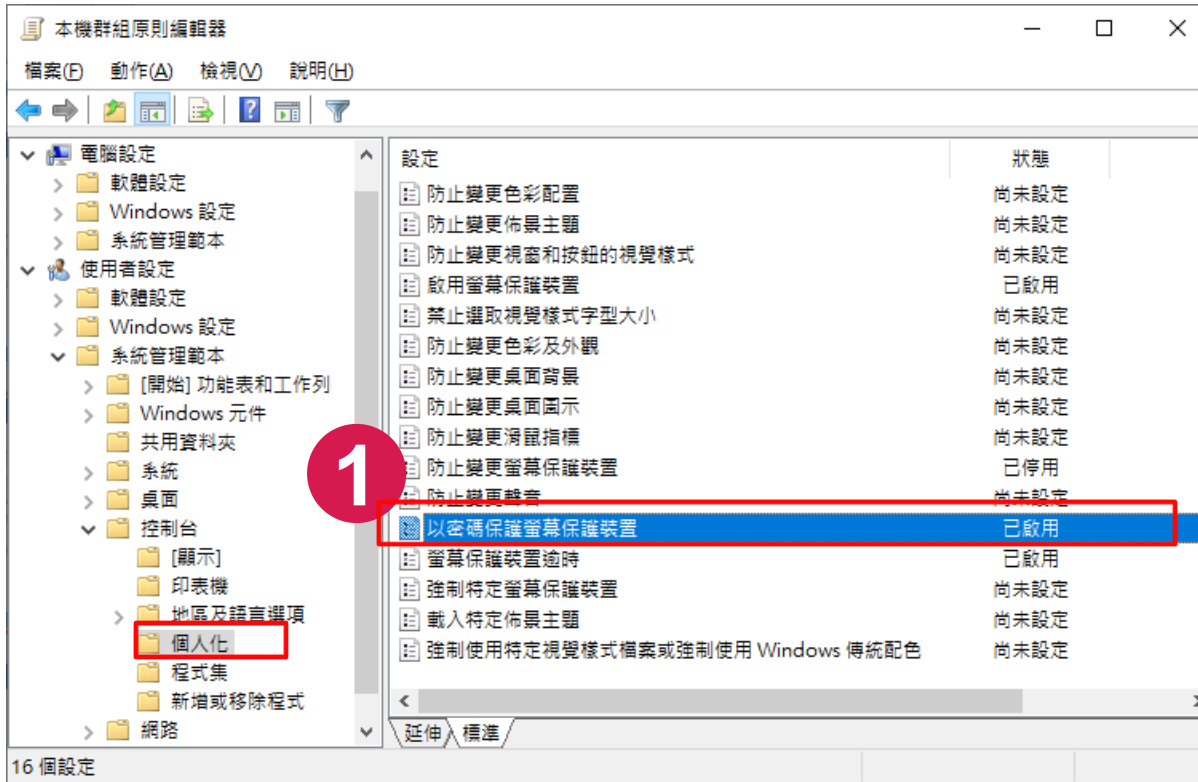
11. 啟用螢幕保護裝置

11. 使用者設定-系統管理範本-控制台-個人化-啟用螢幕保護裝置



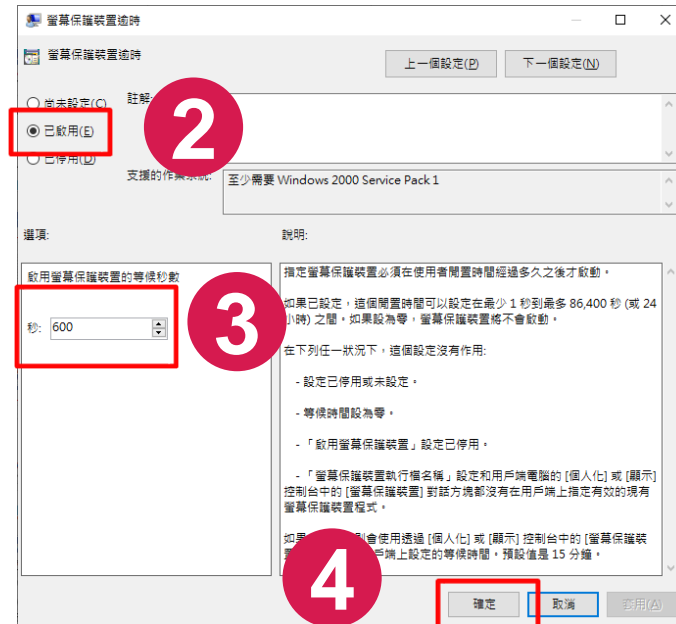
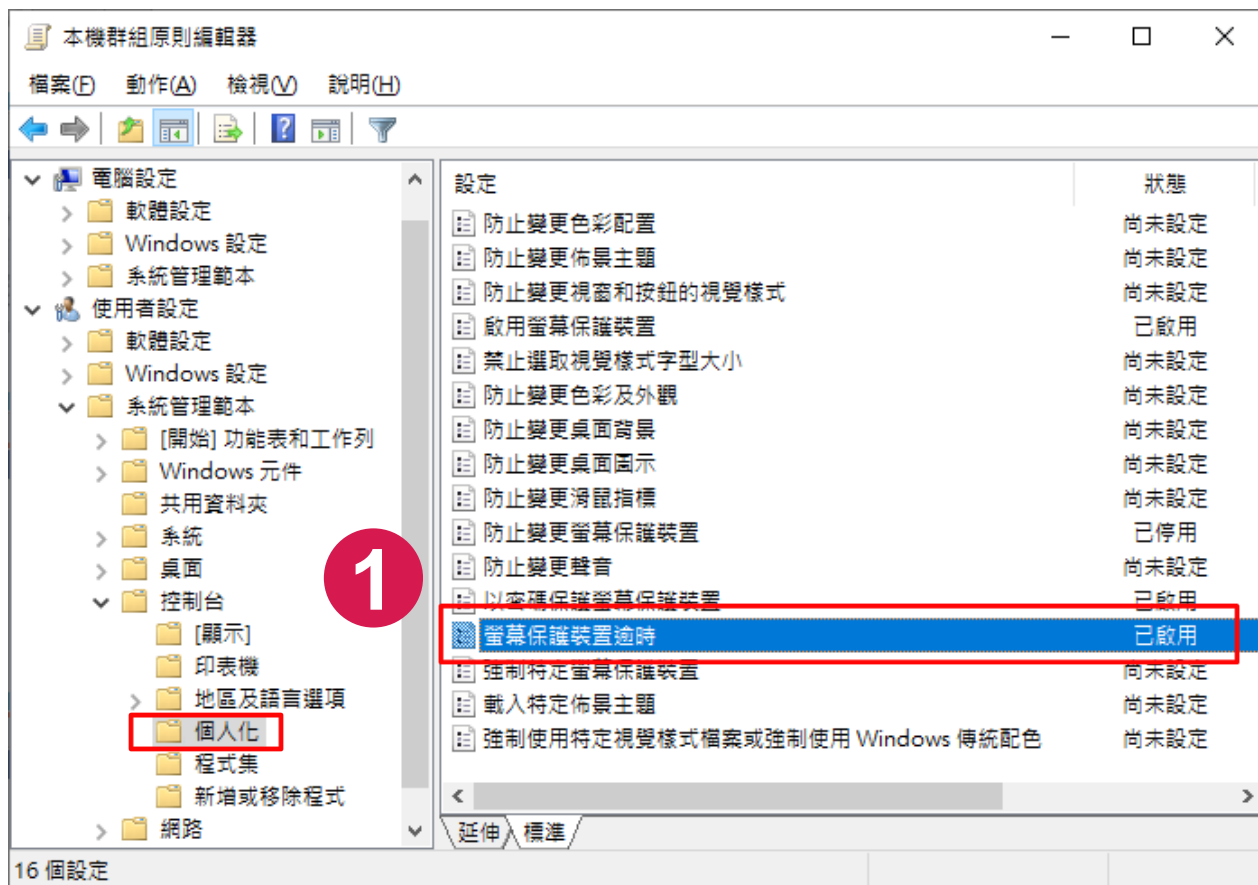
12. 以密碼保護螢幕保護裝置

12. 使用者設定-系統管理範本-控制台-個人化-以密碼保護螢幕保護裝置



13. 螢幕保護裝置逾時

13. 使用者設定-系統管理範本-控制台-個人化-螢幕保護裝置逾時-600秒





三、安裝防毒軟體-以 Trend Apex One 為例



安裝防毒軟體

- 一、安裝前注意事項
- 二、移除舊有的防毒軟體
- 三、安裝防毒軟體與設定定期掃描

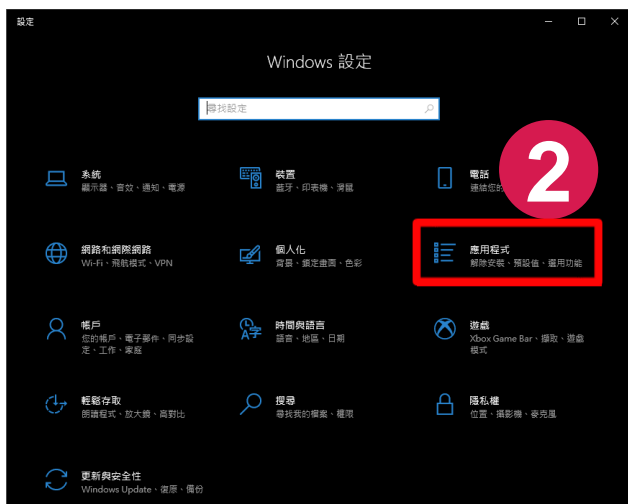
一、安裝前注意事項

- 一、本校採購Trend Apex One，可從校園授權軟體網下載
網址：<https://software.ccu.edu.tw/main.php>
- 二、請先移除舊有防毒軟體重新開機後，再進行新的防毒軟體安裝
- 三、安裝完成後請重新開機

二、移除舊有的防毒軟體

一、從【啟動】→【設定】→【應用程式】→【應用程式與功能】

二、點選防毒軟體的應用程式，點【解除安裝】，移除後請重新開機



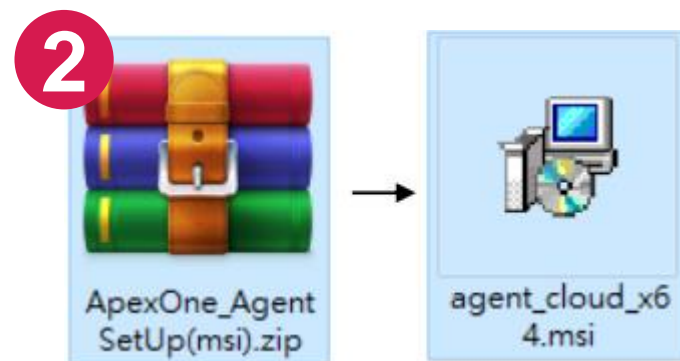
三、安裝防毒軟體與設定定期掃描 1/5

- 一、從校園授權軟體網下載ApexOne防毒軟體
- 二、將檔案解壓縮後對msi檔按滑鼠右鍵，選擇【以系統管理員身分執行】，依程式提示訊息完成安裝

防毒軟體區



軟體名稱	檔案	下載次數
中文版		
▶ ApexOne防毒軟體	Download	1
▶ ApexOne防毒軟體(Mac版本)	Download	
▶ ApexOne安裝手冊	Download	1



使用者帳戶控制

您是否要允許這個來自未知發行者的 App 變更您的裝置?

AgentSetUp_x64.exe

發行者: 未知
檔案來源: 此電腦上的硬碟

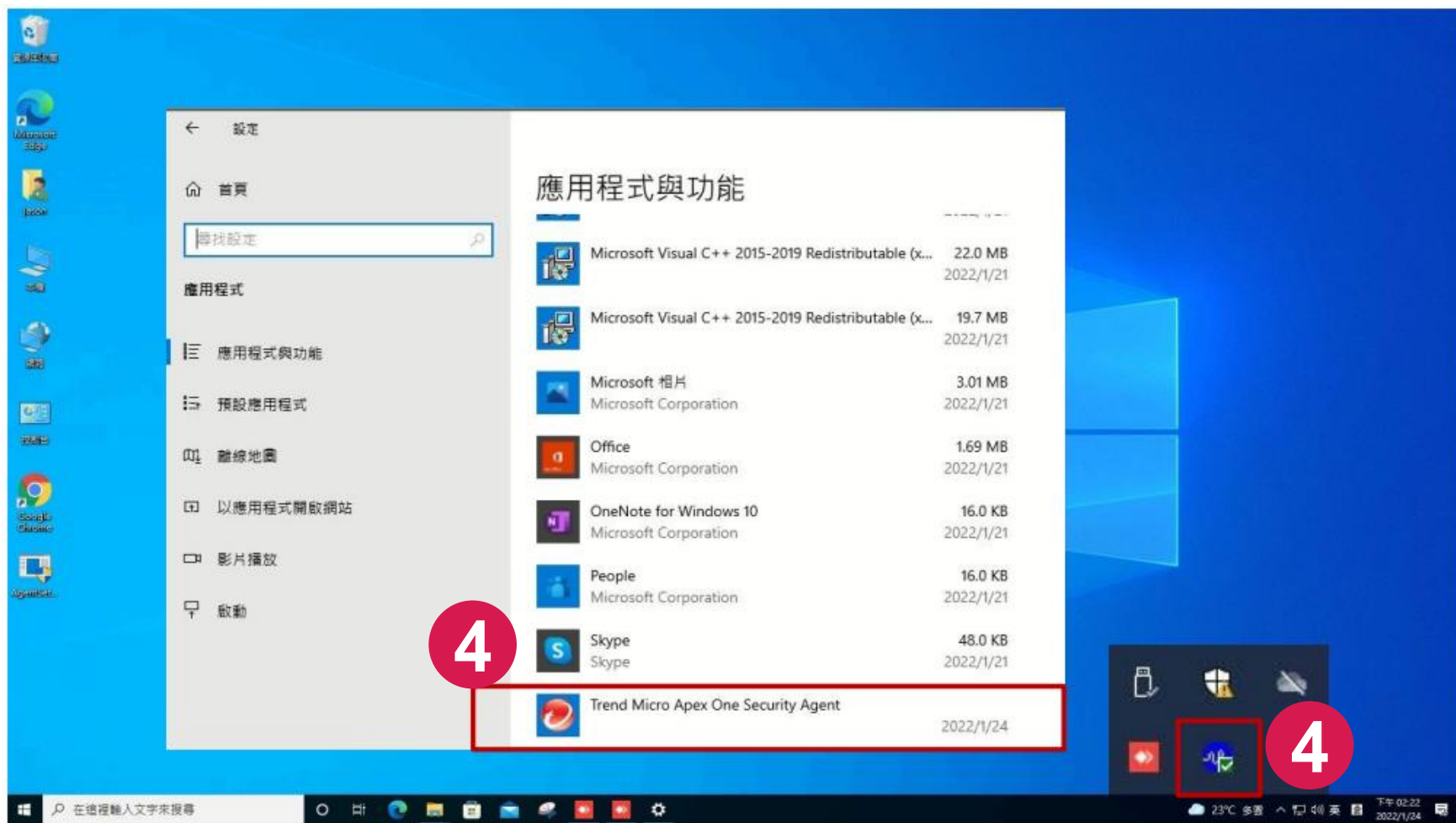
3

更多詳細資料

是 否

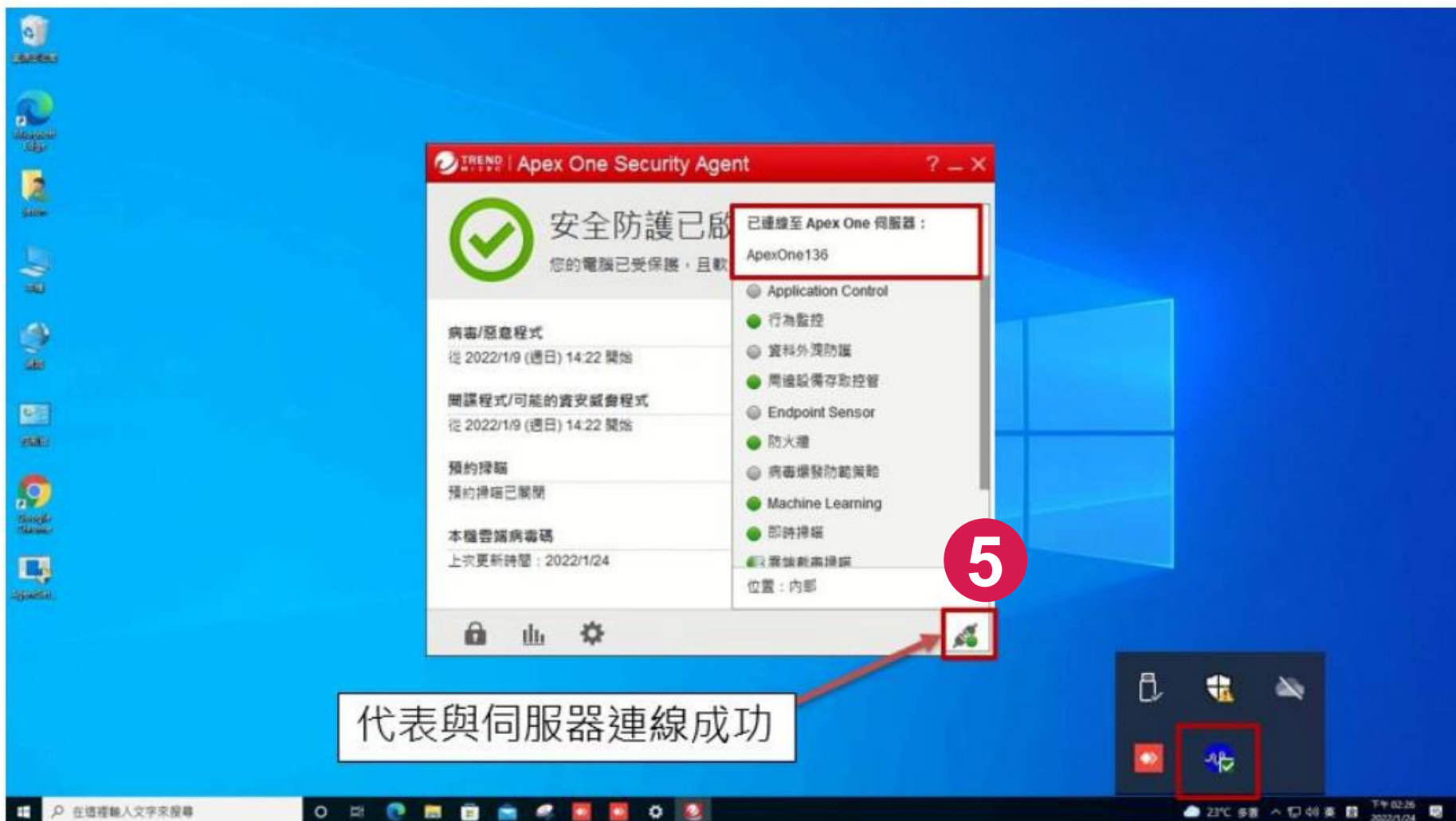
三、安裝防毒軟體與設定定期掃描 2/5

三、等待安裝視窗安裝完成即可看到右下方有產品圖示，也可在【應用程式與功能】檢查是否有檔案



三、安裝防毒軟體與設定定期掃描 3/5

四、點擊圖示並打開服務視窗確認是否連線成功

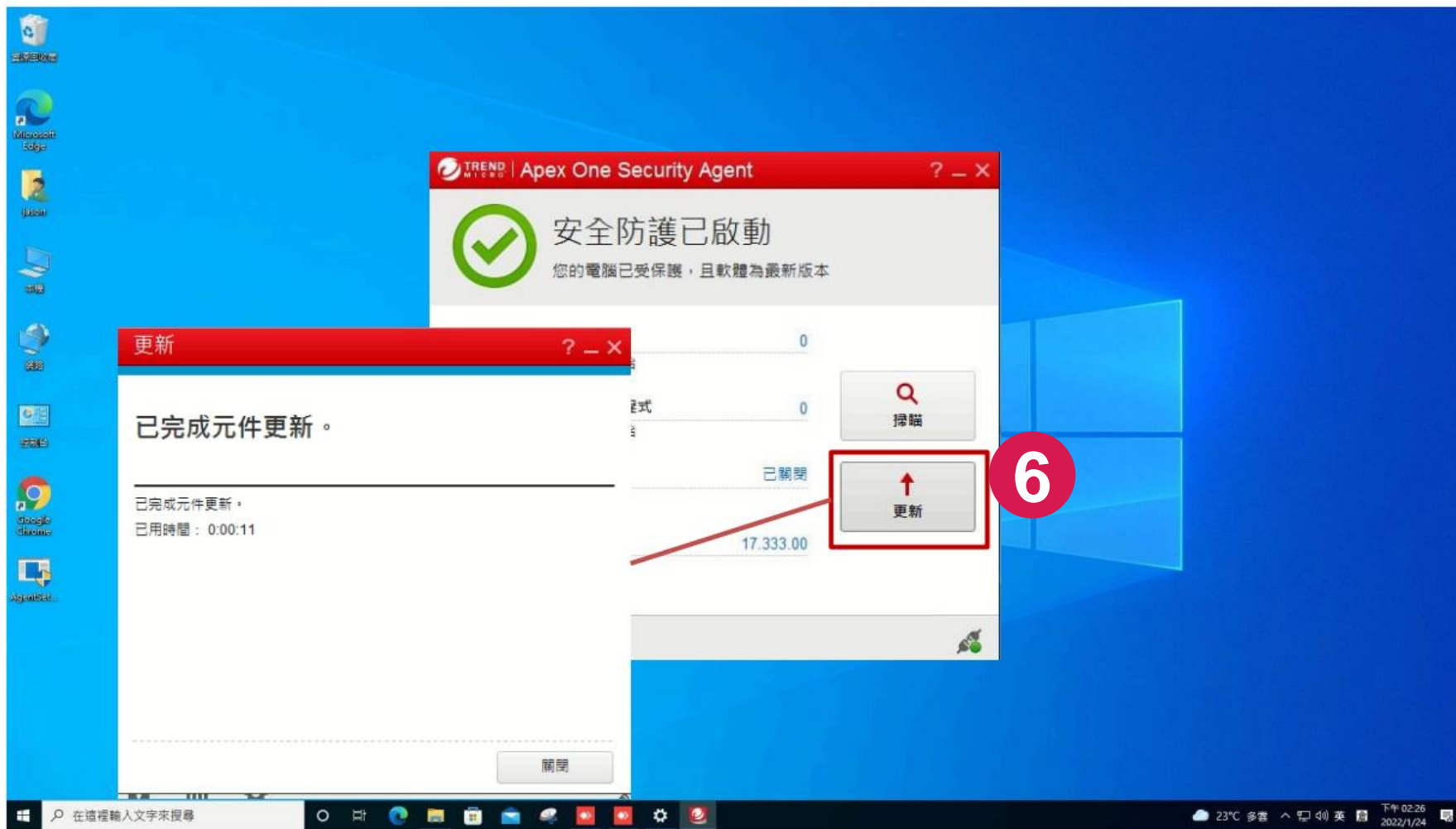


代表與伺服器連線成功

5

三、安裝防毒軟體與設定定期掃描 4/5

五、點擊【更新】，將元件更新至伺服器最新版本




三、安裝防毒軟體與設定定期掃描 5/5

- 六、點擊【解除鎖定】→【已關閉】進入預約掃描設定畫面
- 七、點選【啟動預約掃描】，設定每週掃描一次及時間後，點擊【確定】
- 八、完成設定後重新開機



掃描頻率每週一次
請設定電腦會開機的時間

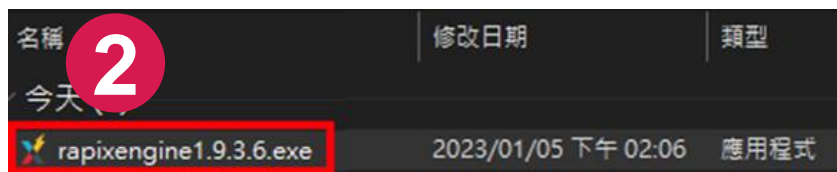
解鎖後才可設定



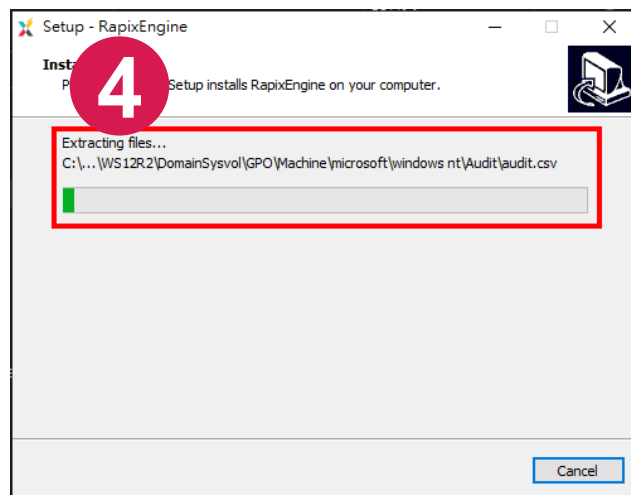
四、安裝資安弱點通報機制(VANS) agent

安裝資安弱點通報機制(VANS) agent 1/2

- 一、請至系統首頁點選圖示下載agent，系統網址：<https://vans.ccu.edu.tw/>
- 二、找到檔案存放目錄，以滑鼠左鍵點選2下執行安裝

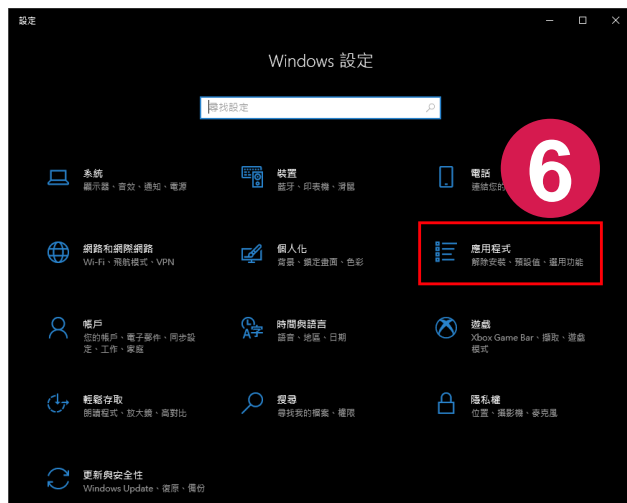
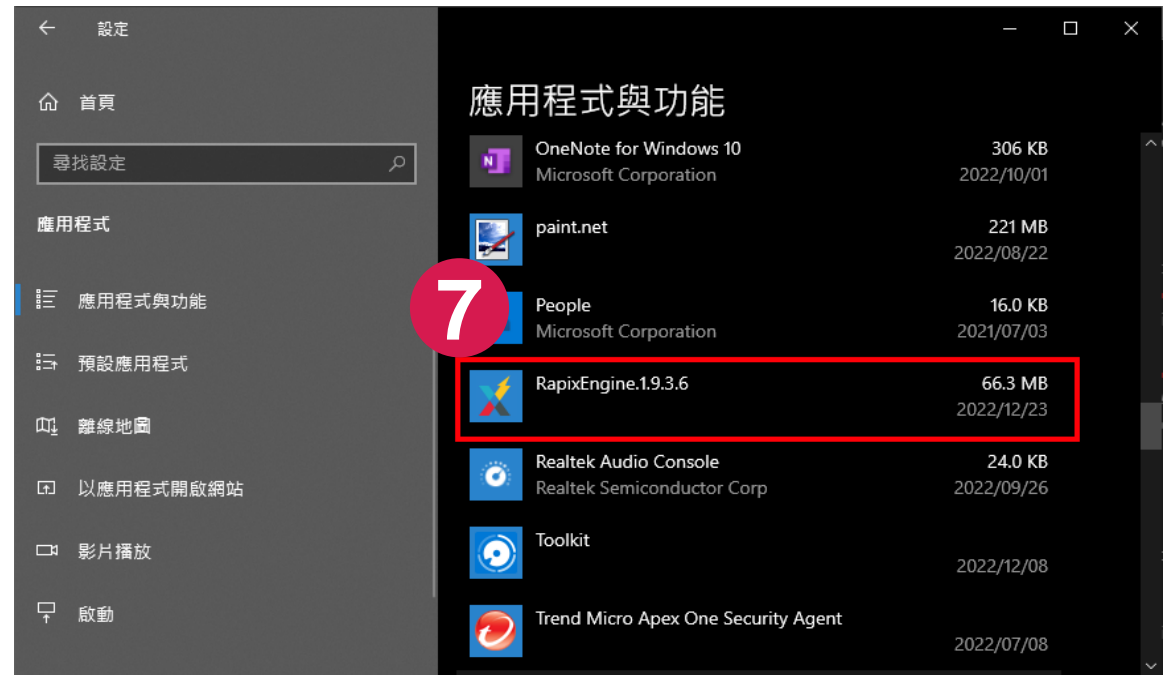


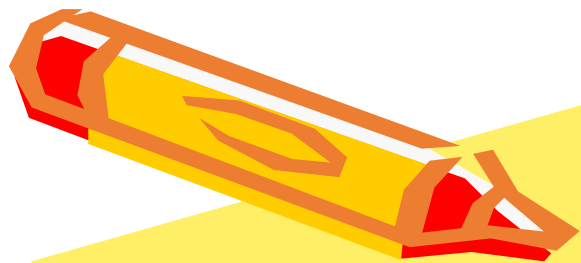
用戶端程式命名為「rapixengine+版本.exe」
以112年1月1.9.3.6版本為例，檔名為「rapixengine1.9.3.6.exe」



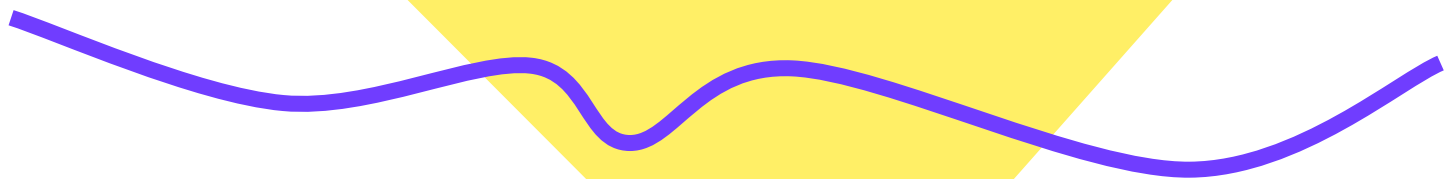
安裝資安弱點通報機制(VANS) agent 2/2

三、成功安裝agent後，可從【啟動】→【設定】→【應用程式】→【應用程式與功能】找到該程式





五、軟體更新設定-以 Windows Office、Adobe Acrobat Reader及7-Zip為例



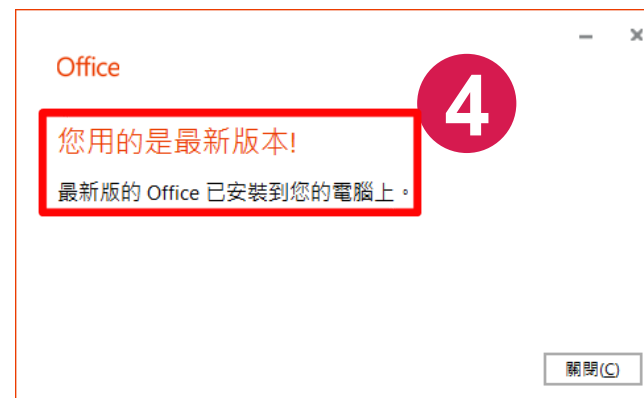
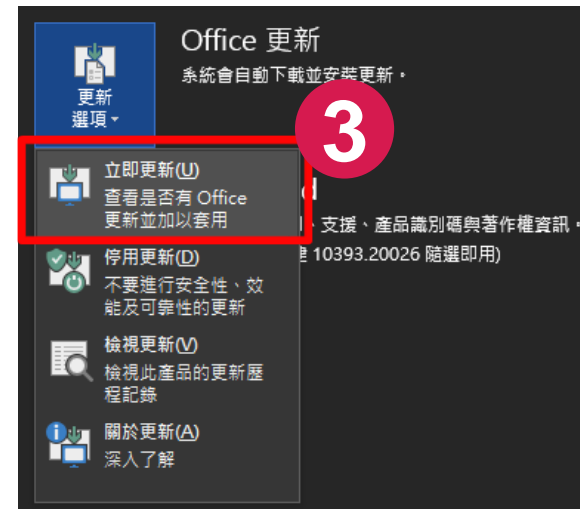
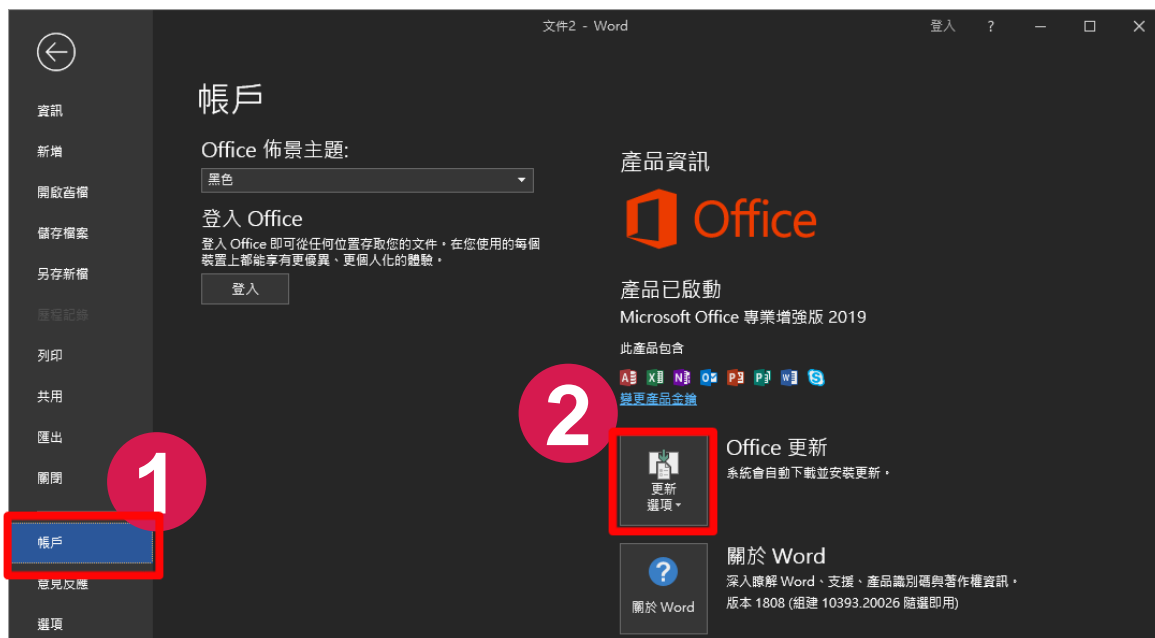
軟體更新設定

- 一、Windows Office
- 二、Adobe Acrobat Reader
- 三、7-Zip

一、Windows Office

一、開啟Word或Excel程式，點選【檔案】→【帳戶】→【更新選項】

二、點選【立即更新】，確認是否已安裝最新版本，如有必要依提示資訊完成安裝



二、Adobe Acrobat Reader

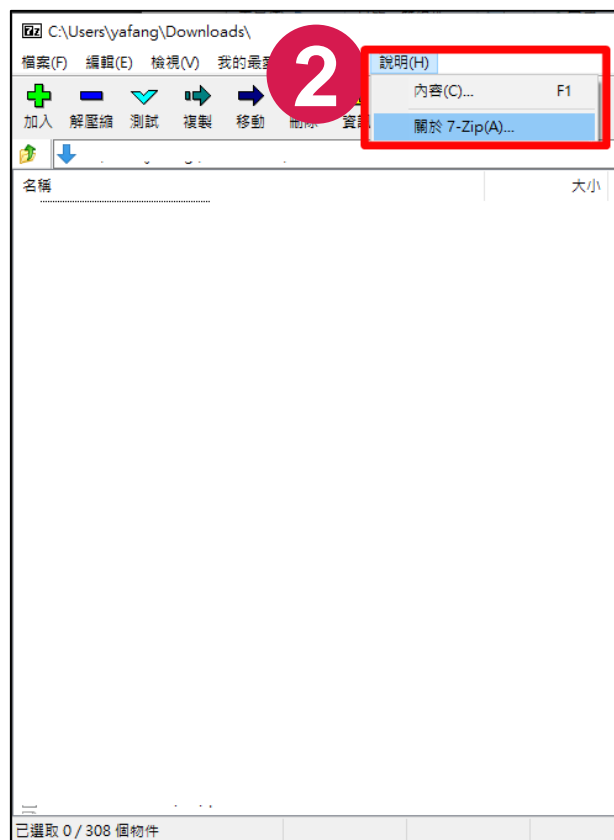
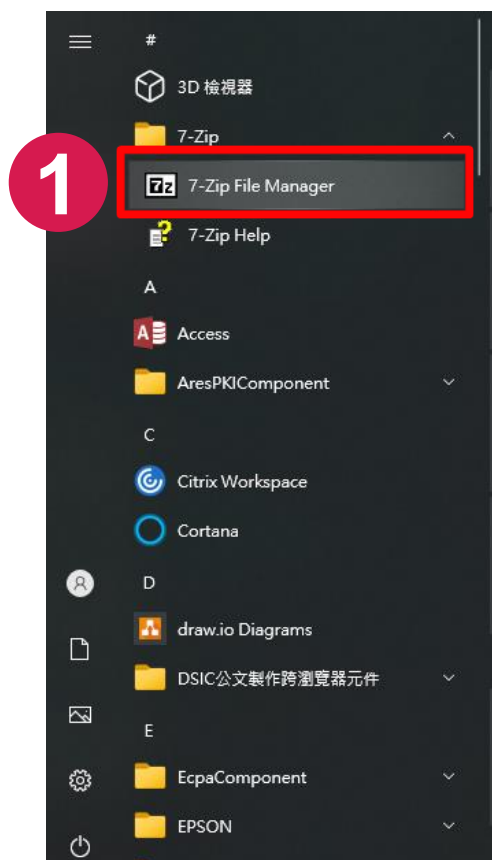
一、開啟Adobe Acrobat Reader程式，點選【說明】→【檢查更新】

二、如有更新可用，點選【下載並安裝】，並依提示資訊完成安裝



三、7-Zip

- 一、點選左下角Windows圖像→【7-Zip File Manager】，開啟程式
- 二、點選【說明】→【關於7-Zip】，確認安裝版本為22.01以上
- 三、如版本太舊，可點選【www.7-zip.org】按鈕至官網下載最新版安裝



THANK
YOU

簡報完畢