

AutoOutlook 教學

一. 下載及安裝

二. 在 Windows 中搜尋 Uac，把安全性降到最低

三. Windows 8 和 Windows 10 徹底降低安全性

開啟「登錄編輯程式」視窗以後，先在左窗格中展開「HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System」，然後在右窗格中找到「EnableLUA」這個 DWORD 值，在上面按一下滑鼠右鍵，跳出選單以後選擇【修改】。

說明：

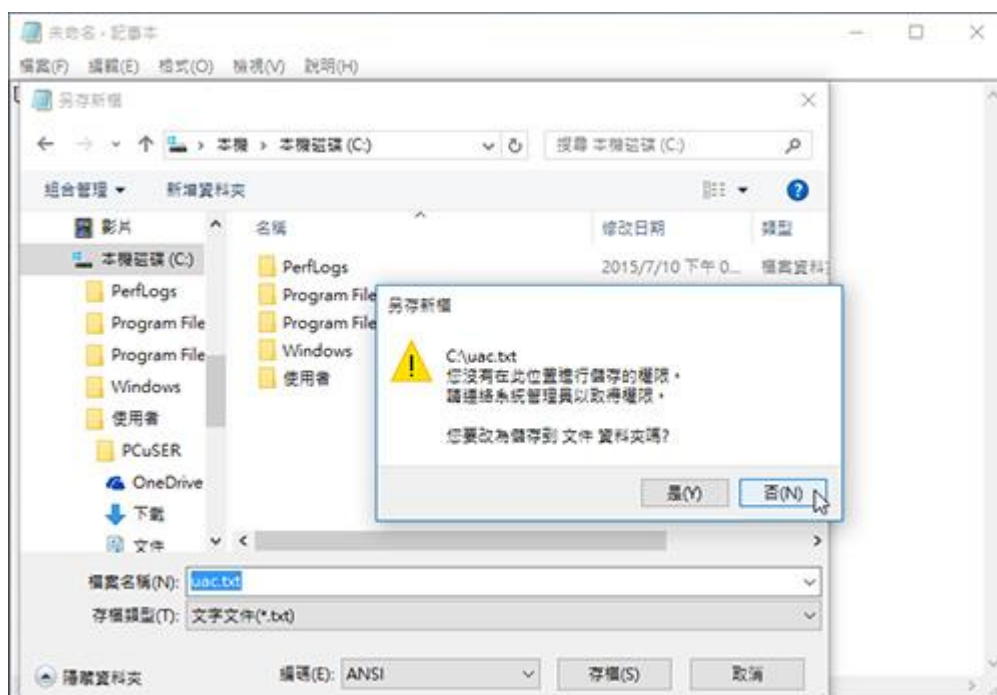
1. 以往在 Win 7 時，我們關閉 UAC 的方式，是進入「使用者帳戶」視窗中按下「變更使用者帳戶控制設定」。



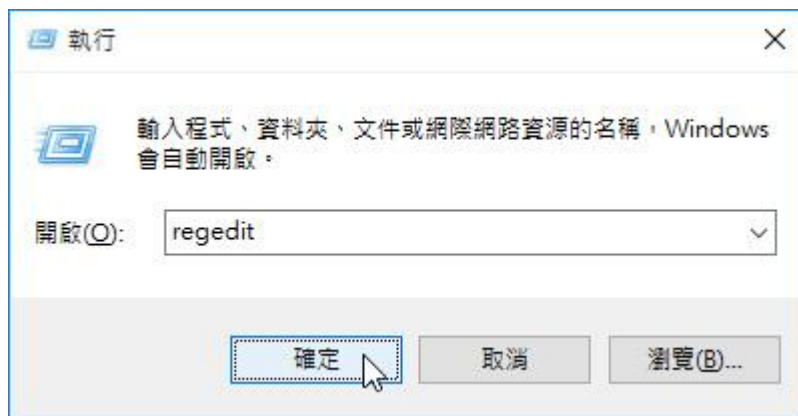
2. 在進入「使用者帳戶控制設定」中，將左方滑桿下拉到「不要通知」，即可變更 UAC 的狀態，在 Windows 10 中也是如此嗎？



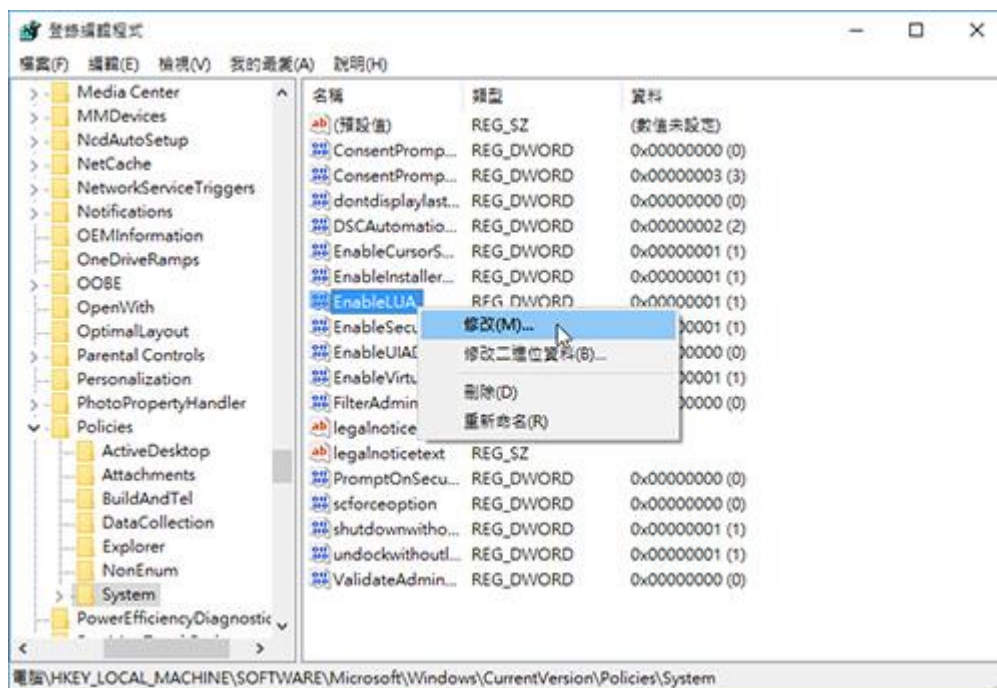
3. 雖然帳號已經是系統管理員，不過在很多軟體需要動到系統設定時，還是會出現問題，這是因為雖然我們已經將 Win 10 的 UAC 關閉，但是實際上就算是 Administrator 帳號也不是最高權限，這是 Win 10 安全性改進的項目之一。



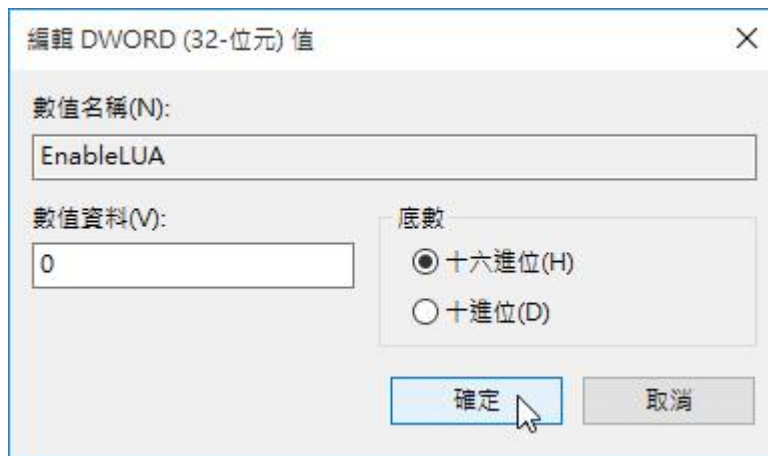
4. 如果要完全關閉 UAC 的話，先要按下鍵盤上的〔開始程式集〕+〔R〕按鍵，叫出「執行」對話盒，然後在空白欄位中輸入「regedit」，然後按一下〔確定〕開啟登錄檔編輯程式。



5. 開啟「登錄編輯程式」視窗以後，先在左窗格中展開「HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System」，然後在右窗格中找到「EnableLUA」這個 DWORD 值，在上面按一下滑鼠右鍵，跳出選單以後選擇【修改】。



6. 開啟編輯對話盒以後，再將「數值資料」欄位更改為「0」，並按下〔確定〕。



7. 這時候可能會在通知區域上跳出提示你要重新啟動電腦的訊息，按一下訊息重新開機。

肆.設定 Outlook 中的 檔案→選項→信任中心→巨集設定和以程式設計方式存取.

如下圖:

一般

郵件

行事曆

連絡人

工作

記事 and 日誌

搜尋

行動訊息

語言

進階

自訂功能區

快速存取工具列

增益集

信任中心

協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。

保護您的隱私權

Microsoft 關心您的隱私權。若需更多關於 Microsoft Outlook 如何保護您的隱私權之資訊，請查看隱私權聲明。

[顯示 Microsoft Outlook 的隱私權聲明](#)

[Office.com 隱私權聲明](#)

[客戶經驗改進計畫](#)

安全性和其他

從 Office.com 了解更多關於保護您的隱私權和安全性的資訊。

[Microsoft 高可信度電腦運算](#)

Microsoft Outlook 信任中心

信任中心包含安全性和隱私權設定。這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定。

信任中心設定(O)...

確定

取消

受信任的執行者

DEP 設定

隱私選項

電子郵件安全性

附件處理

自動下載

巨集設定

以程式設計方式存取

巨集設定

停用所有巨集 (不事先通知)(M)

經過數位簽章的巨集會顯示通知，其他所有巨集會停用(S)

所有巨集都顯示通知(A)

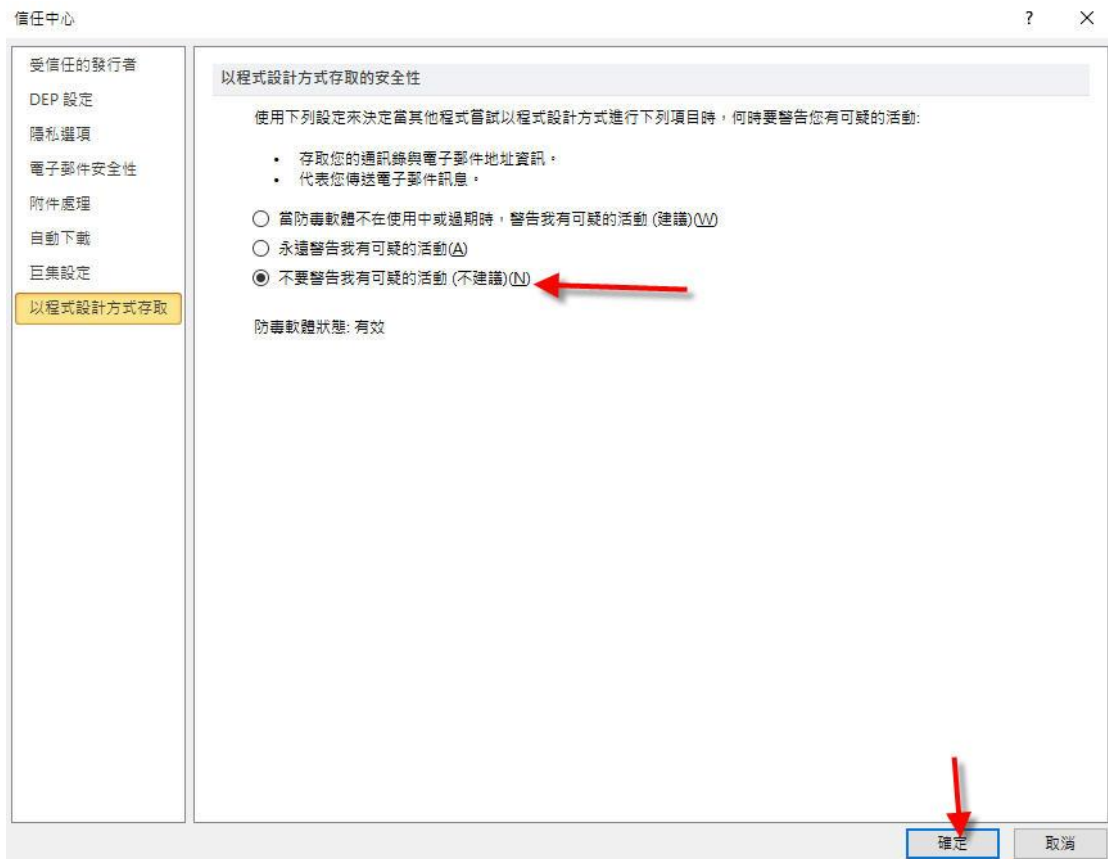
啟用所有巨集 (不建議使用，會執行有潛在危險的程式碼)(D)

增益集

套用巨集安全性設定至安裝的增益集(O)

確定

取消



伍.最後才是 Smtip 的設定
以 gmail 為 server 為例:

1. 要登錄 gmail ,



設定

一般設定 標籤 收件匣 帳戶和匯入 篩選器和封鎖的地址 **轉寄和 POP/IMAP** 外掛程式 即時通訊和視訊會議 進階 離線設定 背景主題

轉寄：
瞭解詳情

停用轉寄
 轉寄外來郵件副本給 並且

驗證

POP 下載：
瞭解詳情

1. 狀態：針對 2019/12/12 起送達的所有郵件啟用 POP 功能
 對所有郵件啟用 POP 功能 (包括已經下載的郵件)
 對現在起所收到的郵件啟用 POP 功能
 停用 POP

2. 當郵件以 POP 存取後

3. 設定電子郵件用戶端 (例如 Outlook、Eudora、Netscape Mail)
[設定說明](#)

接著到 低安全性應用程式和您的 Google 帳戶

<https://support.google.com/accounts/answer/6010255?hl=zh-Hant>

低安全性應用程式和您的 Google 帳戶

如果有人使用不符合 Google 安全標準的應用程式或網站嘗試登入帳戶，我們可能會予以拒絕。低安全性應用程式可能會提高駭客入侵帳戶的機率，因此封鎖這類應用程式的登入活動可協助維護帳戶安全。

如果您的帳戶開啟了「低安全性應用程式存取權」

如果您的帳戶關閉了「低安全性應用程式存取權」

如果您的帳戶關閉了「低安全性應用程式存取權」，您可以重新開啟該設定，但我們建議您改用高安全性應用程式。

← 低安全性應用程式存取權

某些應用程式和裝置採用的登入技術安全性較低，將導致您的帳戶出現安全漏洞。建議您停用這類應用程式的存取權；當然，您也可以選擇啟用存取權，但請瞭解相關風險。如果您並未使用這項設定，Google 會自動關閉該權限。[瞭解詳情](#)

允許低安全性應用程式：已開啟



陸.最後,再到 Outlook 中設定

開啟你的電子郵件程式 (例如 Microsoft Outlook), 然後檢查下列設定。

內送郵件 (POP) 伺服器	pop.gmail.com 需要安全資料傳輸層 (SSL) : 是 通訊埠 : 995
外寄郵件 (SMTP) 伺服器	smtp.gmail.com 需要安全資料傳輸層 (SSL) : 是 需要傳輸層安全性 (TLS) : 是 (如果可用) 需要驗證 : 是 傳輸層安全標準 (TLS)/STARTTLS 通訊埠 : 587 如果你使用的是公司或學校專屬的 Gmail 帳戶, 請洽詢你的 管理員 以取得正確的 SMTP 設定。
伺服器逾時	大於 1 分鐘 (建議設定 5 分鐘)
姓名或顯示名稱	你的姓名
帳戶名稱、使用者名稱或電子郵件地址	你的電子郵件地址
密碼	你的 Gmail 密碼

柒.最後推薦 大量 Email 的傳送,請用 Sendgrid 的服務
www.send.com

app.sendgrid.com 登入.

你會有個帳號及密碼.