



政府組態基準(GCB)實作研習活動

Microsoft Edge

組態設定與實作練習

行政院國家資通安全會報技術服務中心

大綱

- 發展緣由
- 發展目的
- 政府組態基準設定分類
- 政府組態基準設定項目
- 政府組態基準部署說明
- 實作練習

發展緣由

- Microsoft Edge於微軟最新版Windows 10作業系統中取代Internet Explorer成為預設瀏覽器，因此發展Microsoft Edge政府組態基準，並藉由一致性之安全性設定，提升政府機關網頁瀏覽器使用安全性



發展目的

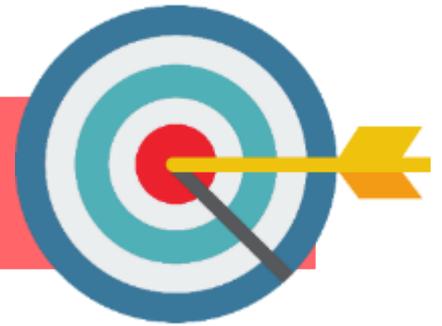
- 針對機關微軟Windows作業系統環境所使用之Edge應用程式進行組態基準設定發展，其目的在於透過GCB的導入，以降低因不安全的設定造成瀏覽器成為駭客入侵管道，進而引發資安事件之疑慮

1

發展一致的安全組態設定

2

提升政府機關瀏覽器使用安全性



政府組態基準設定分類

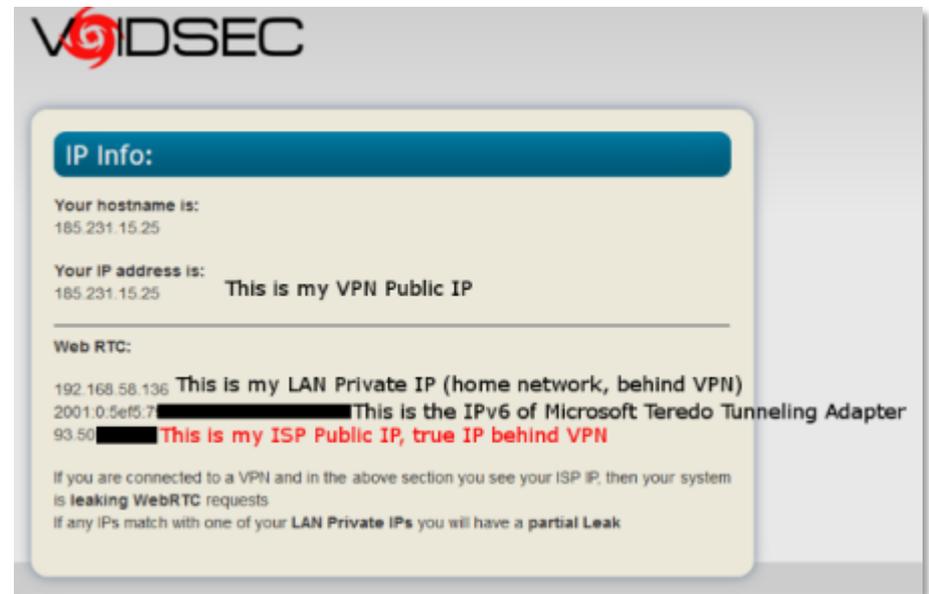
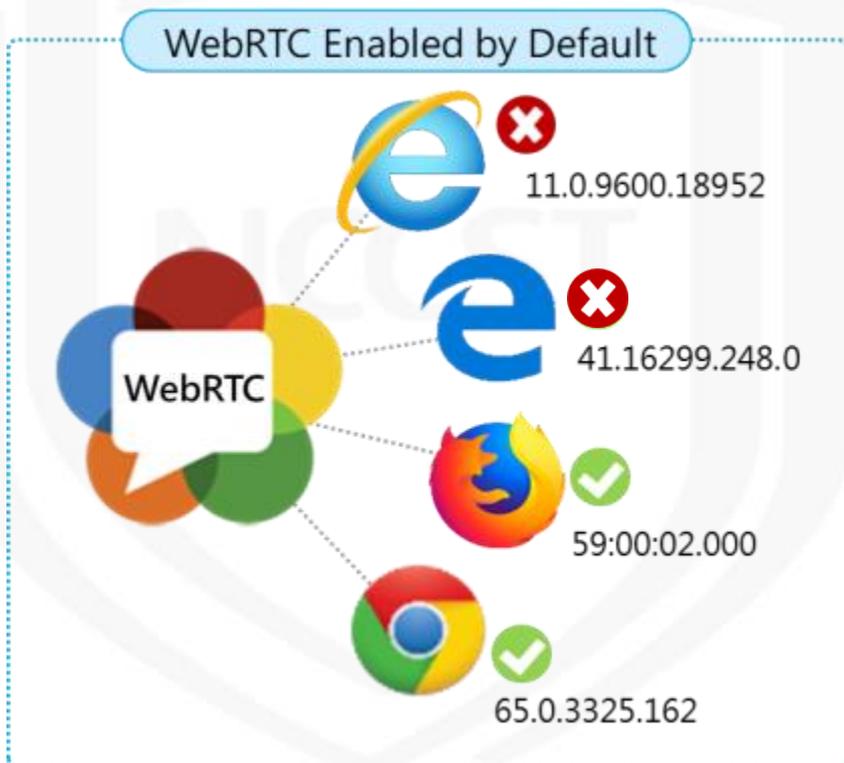
項次	組態基準設定分類	組態基準設定項數
1	安全性和隱私權	8
2	瀏覽器體驗	2
3	擴充功能	1
4	開發人員工具	1
合計		12

政府組態基準設定項目

NCCST

資安事件說明(1/2)

- 外國資安研究員Paolo Stagno於2018年3月發現，市面上有23%的VPN服務，透過瀏覽器的WebRTC技術洩漏使用者真實IP位置，而WebRTC在主流瀏覽器多數是預設啟用的，因此建議停用瀏覽器WebRTC



VOIDSEC

IP Info:

Your hostname is:
185.231.15.25

Your IP address is:
185.231.15.25 **This is my VPN Public IP**

Web RTC:

192.168.58.136 **This is my LAN Private IP (home network, behind VPN)**
2001:0:5ef5:7: [redacted] **This is the IPv6 of Microsoft Teredo Tunneling Adapter**
93.50: [redacted] **This is my ISP Public IP, true IP behind VPN**

If you are connected to a VPN and in the above section you see your ISP IP, then your system is **leaking WebRTC** requests
If any IPs match with one of your LAN Private IPs you will have a **partial Leak**

資安事件說明(2/2)

- 網頁即時通訊(Web Real-Time Communication, WebRTC)
 - 是一個支援網頁瀏覽器進行即時語音對話或影片對話的 API，無需安裝其他外掛程式或第三方軟體，即可讓雙方使用者直接通訊或分享資料。它於2011年6月1日開源並在Google、Mozilla、Opera支援下被納入全球資訊網協會的W3C推薦標準





防止為WebRTC使用Local Host IP位址(1/2)

- 說明

- 這項原則設定決定當使用WebRTC通訊協定撥打電話時，是否要顯示員工的Local Host IP位址

- 若**啟用**此設定，會在使用WebRTC撥打電話時**隱藏**Local Host IP位址

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

防止為WebRTC使用Local Host IP位址(2/2)

● 群組原則設定前與設定後之差異

啟用前

開發人員設定

- 在操作功能表中顯示 [檢視原始檔] 與 [檢查元素]
- 使用 Microsoft 相容性清單
- 使用企業模式網站清單
- 允許 localhost 回送 (這可能會讓您的裝置有風險)。某些狀況 (例如自訂回送主機檔案對應和來自內部網路網站的要求) 可能需要額外設定。如需詳細資訊, 請參閱 [常見問題](#)。
- 允許 Adobe Flash Player localhost 回送 (這可能會使得您的裝置有危險)
- 啟用延伸模組開發人員功能 (這樣可能會危險)
- 為網頁允許不受限制的記憶體使用 (這可整體效能)
- 在 WebRTC 連線上隱藏我的本機 IP 位址
- 啟用觸控式手寫筆導覽和筒狀按鈕選擇

啟用後

開發人員設定

- 在操作功能表中顯示 [檢視原始檔] 與 [檢查元素]
- 使用 Microsoft 相容性清單
- 使用企業模式網站清單
- 允許 localhost 回送 (這可能會讓您的裝置有風險)。某些狀況 (例如自訂回送主機檔案對應和來自內部網路網站的要求) 可能需要額外設定。如需詳細資訊, 請參閱 [常見問題](#)。
- 允許 Adobe Flash Player localhost 回送 (這可能會使得您的裝置有危險)
- 啟用延伸模組開發人員功能 (這樣可能會危險)
- 為網頁允許不受限制的記憶體使用 (這可整體效能)
- 在 WebRTC 連線上隱藏我的本機 IP 位址
- 啟用觸控式手寫筆導覽和筒狀按鈕選擇

資安事件說明

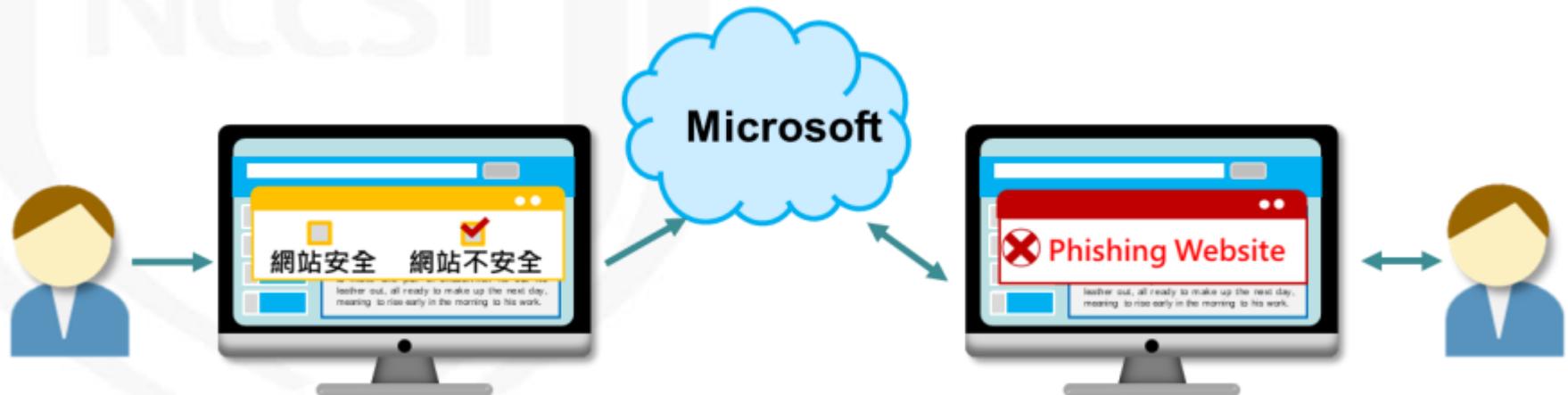
- 趨勢科技在2018年底發布了2019年資安預測報告，以網路釣魚的威脅態勢而言，根據趨勢統計，攔截的網路釣魚相關網址數量逐年攀升，2019年還會更高。隨著行動平臺的盛行，如要針對不同系統開發漏洞攻擊套件變得費工，還要面臨廠商更新修補，因此，社交工程網路釣魚將是網路犯罪者更傾向採用的方式



設定Windows Defender SmartScreen(1/3)

● Windows Defender SmartScreen

- 有助於防止使用者進入Microsoft認定會嘗試竊取個人資訊的詐騙網站與下載惡意軟體。根據報告的網路釣魚網站、惡意程式碼、惡意探索和詐騙網站動態線上清單來檢查網站 (URL)。已下載之檔案的相關資訊，例如檔案的雜湊以及檔案的數位簽章，可以針對線上服務進行檢查，以判斷已下載之程式的評價



設定Windows Defender SmartScreen(2/3)

- 說明

- 這項原則設定決定是否要開啟Windows Defender SmartScreen。Windows Defender SmartScreen可提供警告訊息，避免使用者受到潛在網路釣魚詐騙與惡意軟體的威脅。預設情況下，系統會開啟Windows Defender SmartScreen
- 若啟用此設定，系統會開啟Windows Defender SmartScreen，使用者無法關閉

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

設定Windows Defender SmartScreen(3/3)

● 群組原則設定前與設定後之差異

啟用前



雖看似未設定，但微軟預設為啟用

啟用後



防止略過網站的Windows Defender SmartScreen提示(1/2)



- 說明

- 這項原則設定決定使用者是否可以覆寫有關潛在惡意網站的Windows Defender SmartScreen警告
- 若啟用此設定，使用者無法略過Windows Defender SmartScreen警告，且系統會防止使用者繼續瀏覽該網站

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

防止略過網站的Windows Defender SmartScreen提示(2/2)



● 群組原則設定前與設定後之差異

啟用前

已報告此網站為不安全
已託管 nav.smartscreen.msft.net

我們建議您不要繼續瀏覽此網站。已有使用者向 Microsoft 回報此網站包含會對電腦造成風險的威脅，此威脅可能會造成個人或財務資訊洩漏。

返回安全性

其他資訊

已有使用者報告此網站包含下列威脅：

- 網路釣魚威脅: 這是一個網路釣魚網站，可能誘使您提供個人或財務資訊。

> 報告此網站並未包含威脅
> 略過並繼續 (不建議)

Windows Defender SmartScreen

使用者可略過警告繼續執行

啟用後

已報告此網站為不安全
已託管 nav.smartscreen.msft.net

我們建議您不要繼續瀏覽此網站。已有使用者向 Microsoft 回報此網站包含會對電腦造成風險的威脅，此威脅可能會造成個人或財務資訊洩漏。

返回安全性

其他資訊

已有使用者報告此網站包含下列威脅：

- 網路釣魚威脅: 這是一個網路釣魚網站，可能誘使您提供個人或財務資訊。

> 報告此網站並未包含威脅

Windows Defender SmartScreen

使用者無法繼續執行

防止略過檔案的Windows Defender SmartScreen提示



- 說明

- 這項原則設定決定使用者是否可覆寫有關下載未經驗證之檔案的Windows Defender SmartScreen警告
- 若啟用此設定，使用者無法略過Windows Defender SmartScreen警告，且系統會防止使用者繼續下載未經驗證的檔案

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

資安事件說明

- 2018年12月，軟體開發商Phoenix Technologies的研究人員Bruno Keith公布Microsoft Edge漏洞的攻擊程式，此漏洞編號為CVE-2018-8629漏洞。當Edge所使用的JavaScript引擎Chakra不當處理記憶體中的物件時，即會觸發該漏洞，駭客可架設一個惡意網站或是滲透正當網站誘導Edge使用者造訪，成功的開採即允許駭客取得使用者權限，包含安裝或移除程式、更改或刪除資料，以及建立帳號，掌控被駭系統



設定密碼管理員(1/3)

- 說明

- 這項原則設定決定使用者是否可以使用「密碼管理員」在本機儲存其密碼。預設情況下，系統會開啟「密碼管理員」
- 若停用此設定，使用者無法使用「密碼管理員」在本機儲存其密碼

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

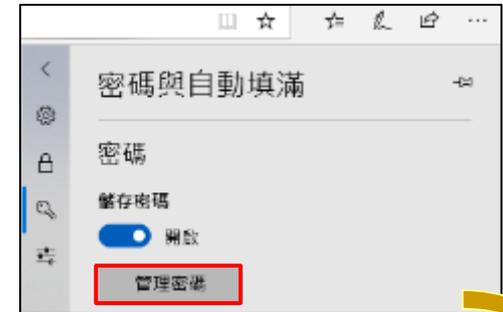
- 建議值

- 停用

設定密碼管理員(2/3)

● 群組原則設定前與設定後之差異

停用前



停用後



設定密碼管理員(3/3)

- 群組原則設定前與設定後之差異

控制台 > 使用者帳戶 > 認證管理員

管理您的認證
檢視與刪除網站、連線的應用程式及網路的已儲存登入資訊。

網站認證

Windows 認證

網站密碼

https://www.facebook.com/ gcbtest@gmail.com

網址 (URL): https://www.facebook.com/
使用者名稱: gcbtest@gmail.com
漫遊: 是
存檔者: Internet Explorer
密碼: **顯示**
移除

Windows 安全性

請驗證您的認證，以檢視儲存的密碼

USER

.....

DESKTOP-884F99T\USER

Caps Lock 已啟用

其他選擇

確定 取消

網站密碼

https://www.facebook.com/ gcbtest@gmail.com

網址 (URL): https://www.facebook.com/
使用者名稱: gcbtest@gmail.com
漫遊: 是
存檔者: Internet Explorer
密碼: 12345678 隱藏
移除

當使用者電腦的帳號密碼外洩時，透過Edge所儲存的帳號密碼也面臨外洩風險

資安事件說明

- 內政部警政署發布防詐騙警訊，2019年6月出現常見的抽獎詐騙網頁惡意彈跳視窗，無論在Android、iOS系統或是電腦版網頁上都會出現，讓使用者誤以為真的中獎，而掉入詐騙陷阱。網頁跳出廣告通知中獎的詐騙手法，內容會隨著更新為目前市面上最新版的手機，並提出小問題，目的就是要竊取個人資料

小心
詐騙



設定快顯封鎖程式(1/2)

- 說明

- 這項原則設定決定是否要開啟「快顯封鎖程式」。預設情況下，系統會開啟「快顯封鎖程式」
- 若啟用此設定，系統會開啟「快顯封鎖程式」以防止顯示快顯視窗

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

設定快顯封鎖程式(2/2)

- 群組原則設定前與設定後之差異

啟用後

PopupTest 1
This page will launch a total of 10 popup windows

Loading Popup windows.

Done!

If you didn't see any popup windows, you are probably using a popup blocker and it is working.
Or, you are using a non-standard browser...
Or, you have Java turned off...

BACK

允許 'http://www.popupstest.com/popup1.html'
允許 'http://www.popupstest.com/popup2.html'
允許 'http://www.popupstest.com/popup3.html'
允許 'http://www.popupstest.com/popup4.html'
允許 'http://www.popupstest.com/popup5.html'
允許 'http://www.popupstest.com/popup6.html'
允許所有快顯

Microsoft Edge 已封鎖來自 www.popupstest.com 的快顯。
允許一次 ^ 一律允許

阻擋快顯視窗

微軟預設情況下，系統會開啟「快顯封鎖程式」

若關閉

PopupTest 1
This page will launch a total of 10 popup windows

Loading Popup windows...

Done!

If you didn't see any popup windows, you are probably using a popup blocker and it is working.
Or, you are using a non-standard browser...
Or, you have Java turned off...

BACK

允許顯示快顯視窗

PopupTest Friday October, 04 2019 - Microsoft Edge

www.popupstest.com/popup4.html

Pop-up

資安事件說明

- 2018年3月爆發的劍橋分析醜聞，不當取得臉書8,700多萬用戶的個資。當用戶授權活動資訊的API後，第三方就能存取用戶個資、數位足跡及個人喜好等，且開發人員還能一併取得這些用戶好友們的各種資料，而不需要進一步獲得這群好友的授權，因此停用第三方cookie將可降低使用者行為等資訊被他人蒐集之風險



設定Cookie(1/2)

- 說明

- 這項原則設定決定處理Cookie的方式

- 若啟用此設定，必須決定是否要：

- 允許所有Cookie(預設值)：允許所有網站的所有Cookie

- 封鎖所有Cookie：封鎖來自所有網站的Cookie

- 只封鎖第三方Cookie：只封鎖來自第三方網站的Cookie

- 設定路徑

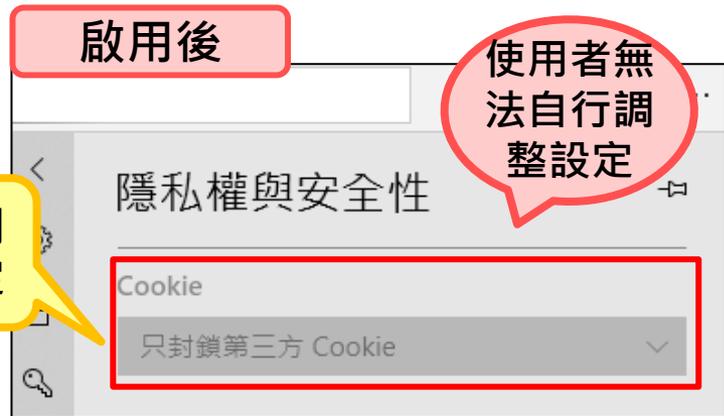
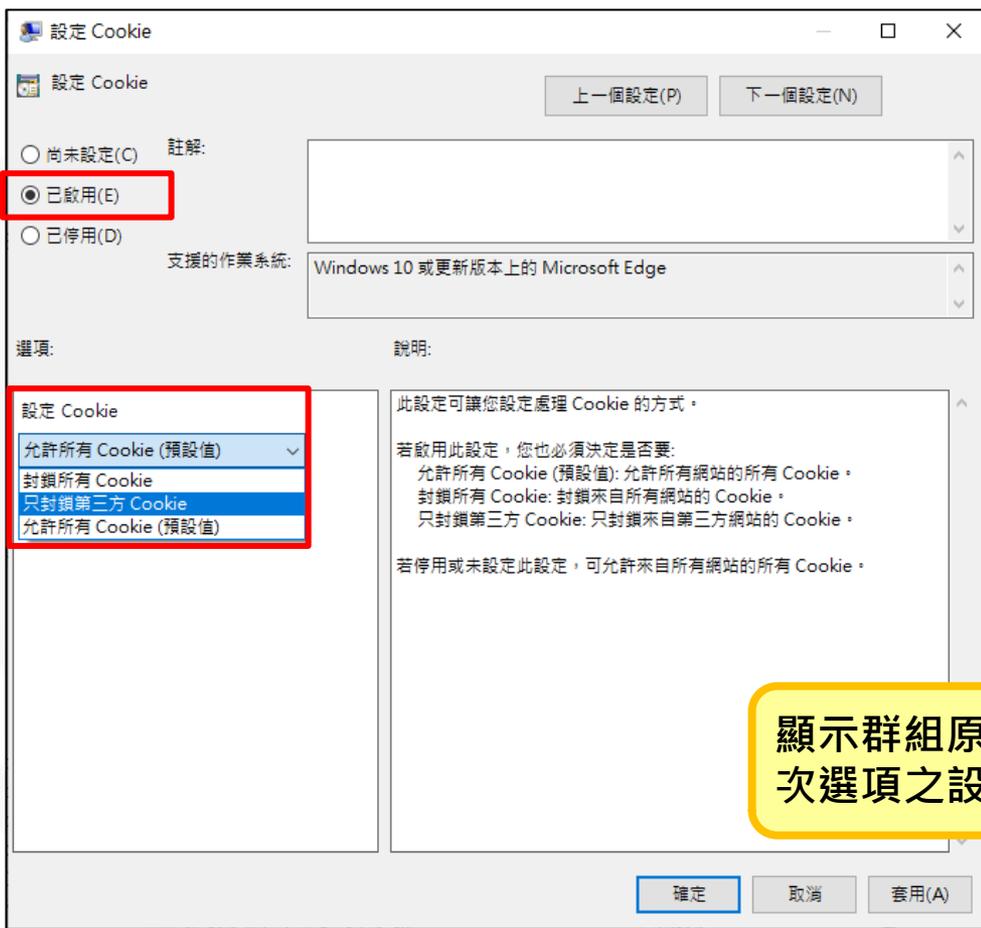
- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用，只封鎖第三方Cookie

設定Cookie(2/2)

● 群組原則設定前與設定後之差異



資安事件說明

- 芬蘭的網頁開發人員Viljami Kuosmanen於2017年1月發現，包括Chrome與Safari等瀏覽器的自動填入 (autofill)功能暗藏網釣風險，可能會曝露未經使用者同意的個人資訊。駭客透過藏匿表格資訊，看起來只要求使用者填入姓名及電子郵件，實際上卻可獲得使用者所儲存的所有個資，例如國別、地址、電話號碼等資訊

使用者看到的介面



Name	<input type="text"/>
Email	<input type="text"/>
<input type="submit" value="Submit"/>	

自動填入

自動填入

真實介面含有隱藏欄位

Name	<input type="text"/>	Phone	<input type="text"/>	Address	<input type="text"/>
Email	<input type="text"/>	Country	<input type="text"/>	Credit Card	<input type="text"/>
<input type="submit" value="Submit"/>					

一併自動填入



設定自動填寫(1/2)

- 說明

- 這項原則設定決定使用者是否可以在使用Microsoft Edge時，使用「自動填寫」來自動填寫表單欄位。預設情況下，使用者可以選擇是否要使用「自動填寫」
- 若停用此設定，使用者無法在使用Microsoft Edge時，使用「自動填寫」來自動填寫表單

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 停用

設定自動填寫(2/2)

- 群組原則設定前與設定後之差異

停用前

密碼與自動填寫

自動填寫

儲存表單資料

開啟

管理表單

使用者可自行管理儲存資訊

管理表單

chen Joe
台北市大安區富陽街116號, 台北市....
nccst@nat.gov.tw
0227391000

新增一個新的

匯出

停用後，已儲存的資訊不會刪除

停用後

密碼與自動填寫

部分設定是由您的組織所管理

自動填寫

儲存表單資料

關閉

使用者無法自行更改

範例

Name	chen Joe
Email	nccst@nat.gov.tw
Submit	

Name	Your Name
chen Joe	nccst@nat.gov.tw
管理表單	

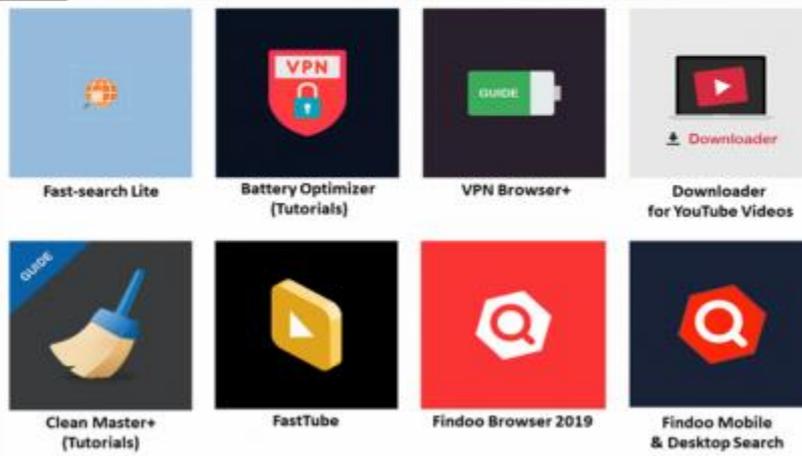
使用者看到的輸入欄位，使用自動填入

```
{  
  "args": {},  
  "data": "",  
  "files": {},  
  "form": {  
    "address": "\u53f0\u5317\u5e02\u5927\u5b89\u5340\u5bcc\u967d\u8857116\u865f",  
    "cc_cv": "",  
    "cc_month": "01",  
    "cc_number": "",  
    "cc_year": "2017",  
    "city": "\u53f0\u5317\u5e02",  
    "country": "",  
    "email": "nccst@nat.gov.tw",  
    "name": "chen Joe",  
    "organization": "\u6280\u8853\u670d\u52d9\u4e2d\u5fc3",  
    "phone": "0227391000",  
    "postal": "10676"  
  }  
}
```

使用自動填入隱藏欄位藉機取得資訊

資安事件說明

- 賽門鐵克在2019年1月於微軟官方案式市集 Microsoft Store中發現了8款程式，這些看似正常的合法程式卻藏有挖礦機制，可利用使用者的電腦資源來開採門羅幣(Monero)，這些程式可在Windows 10上執行，且在程式的描述中完全未提及挖礦功能



install



允許延伸模組(1/2)

- 說明

- 這項原則設定決定使用者是否可以在Microsoft Edge中載入延伸模組
- 若停用此設定，使用者無法使用Edge延伸模組

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

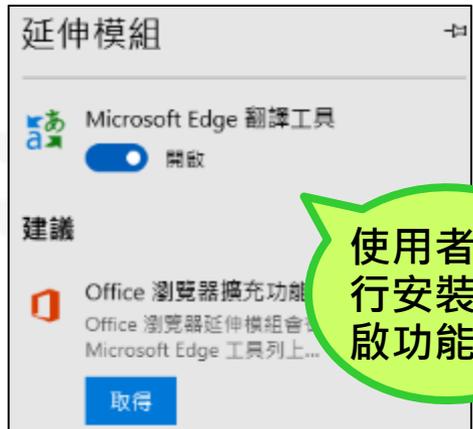
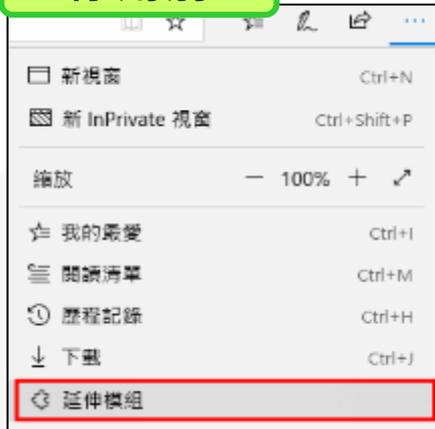
- 建議值

- 停用

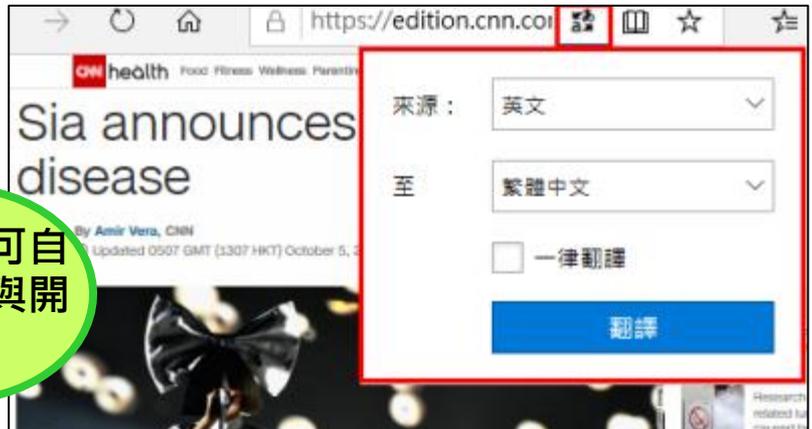
允許延伸模組(2/2)

- 群組原則設定前與設定後之差異

停用前



使用者可自行安裝與開啟功能



停用後



使用者無法自行更改

防止在Microsoft Edge中存取about:flags頁面 (1/2)



- 說明

- 這項原則設定決定使用者是否能存取about:flags頁面，此頁面是用來變更開發人員設定或啟用實驗性功能
- 若啟用此設定，使用者將無法存取about:flags頁面

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

防止在Microsoft Edge中存取about:flags頁面 (2/2)



● 群組原則設定前與設定後之差異

啟用前

開發人員設定

- 在操作功能表中顯示 [檢視原始檔] 與 [檢查元素]
- 使用 Microsoft 相容性清單
- 使用企業模式網站清單
- 允許 localhost 回送 (這可能會讓您的裝置有風險)。某些狀況 (例如自訂回送主機檔案對應和來自內部網路網站的要求) 可能需要額外設定。如需詳細資訊，請參閱[常見問題](#)。
- 允許 Adobe Flash Player localhost 回送 (這可能會使得您的裝置有危險)
- 啟用延伸模組開發人員功能 (這樣可能會讓您的裝置有風險)
- 為網頁允許不受限制的記憶體使用 (這可能會影響裝置的整體效能)
- 在 WebRTC 連線上隱藏我的本機 IP 位址
- 啟用觸控式手寫筆導覽和筒狀按鈕選擇

啟用後

您無法存取此頁面

您的組織不允許它

使用者無法自行更改

使用者可
自行勾選
選項

允許InPrivate瀏覽(1/2)

- 說明

- 這項原則設定決定使用者是否可使用InPrivate網站瀏覽功能進行瀏覽
- 停用此設定，使用者無法使用InPrivate網站瀏覽功能

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 停用

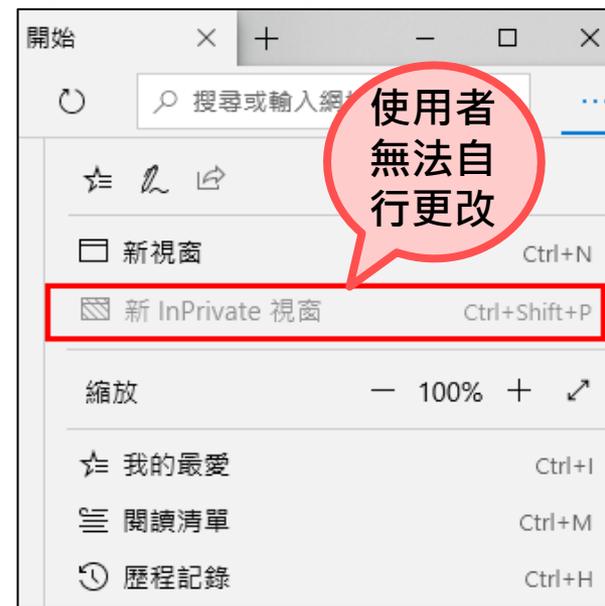
允許InPrivate瀏覽(2/2)

- 群組原則設定前與設定後之差異

停用前



停用後



設定「不要追蹤」(1/2)

- 說明

- 這項原則設定決定使用者是否可以傳送「不要追蹤」的註記到要求追蹤資訊的網站。預設情況下，系統不會傳送「不要追蹤」註記，但使用者可以選擇開啟並傳送註記
- 若啟用此設定，系統一律會傳送「不要追蹤」的註記到要求追蹤資訊的網站

- 設定路徑

- 電腦設定\系統管理範本\電腦元件\Microsoft Edge

- 建議值

- 啟用

設定「不要追蹤」(2/2)

- 群組原則設定前與設定後之差異

啟用前



啟用後



政府組態基準部署說明

NCCST

AD環境部署說明

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the acronym "NCCST" inside.

安裝Microsoft Edge 系統管理範本

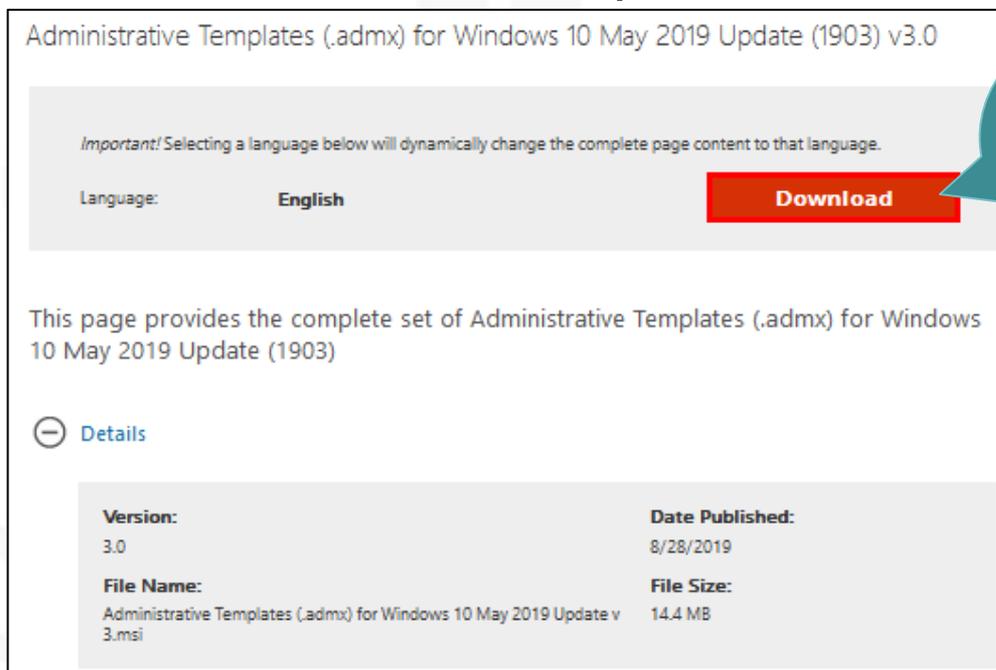
NCCST

安裝Microsoft Edge系統管理範本(1/3)

- Microsoft Edge系統管理範本說明

- Microsoft Edge系統管理範本提供了Windows 10內建Edge瀏覽器之群組原則與設定路徑

- 下載位置：<https://www.microsoft.com/en-us/download/details.aspx?id=58495>



Administrative Templates (.adm) for Windows 10 May 2019 Update (1903) v3.0

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English** **Download**

This page provides the complete set of Administrative Templates (.adm) for Windows 10 May 2019 Update (1903)

⊖ Details

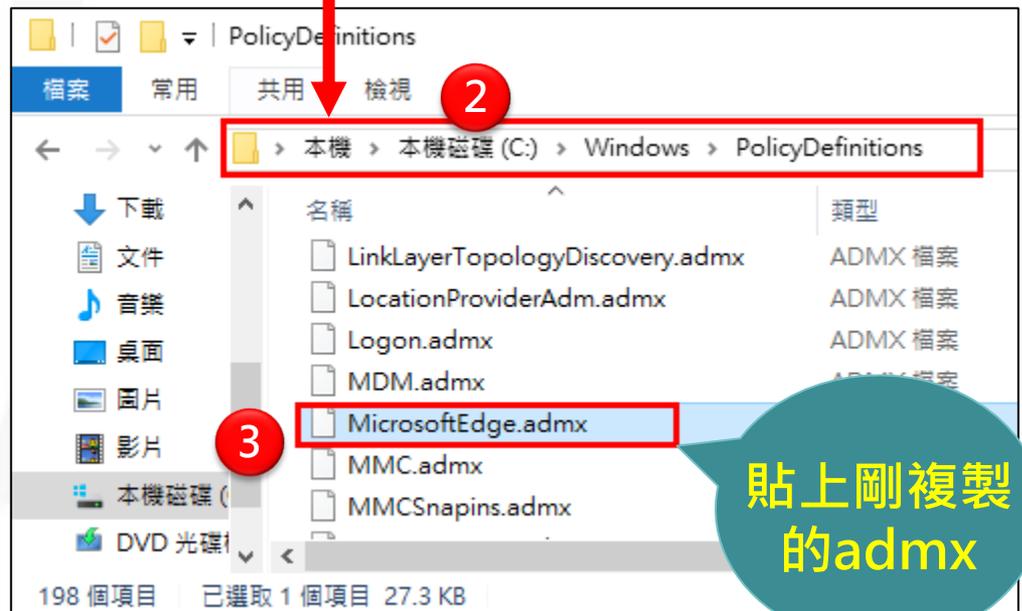
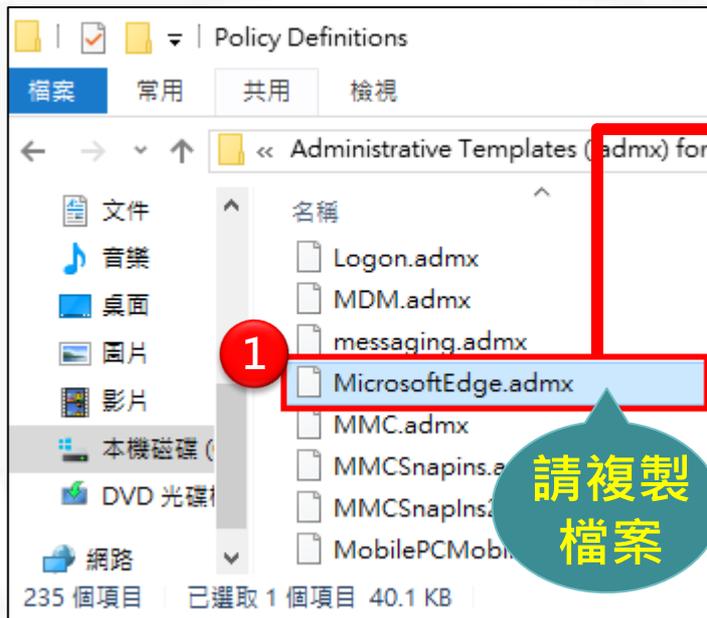
Version:	Date Published:
3.0	8/28/2019
File Name:	File Size:
Administrative Templates (.adm) for Windows 10 May 2019 Update v3.msi	14.4 MB

請點選此處會自動下載

安裝Microsoft Edge系統管理範本(2/3)

● Microsoft Edge系統管理範本安裝方式

- 將下載的檔案解壓縮，並複製MicrosoftEdge.admx檔案至「C:\Windows\PolicyDefinitions」



安裝Microsoft Edge系統管理範本(3/3)

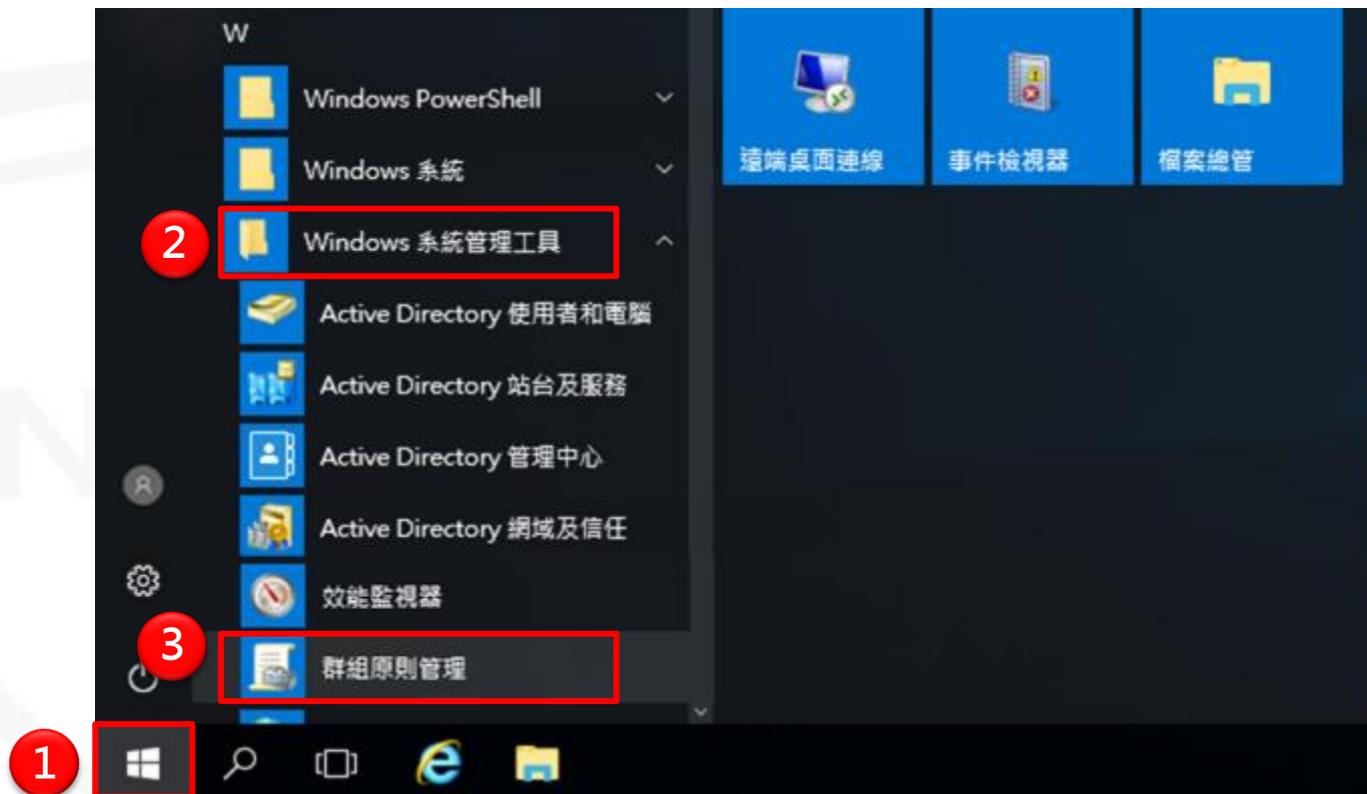
- Microsoft Edge系統管理範本安裝方式

- 將下載的檔案解壓縮，並複製MicrosoftEdge.adml檔案至「C:\Windows\PolicyDefinitions\zh-TW」



AD環境下的導入方式(1/6)

- 點擊開始→Windows系統管理工具→群組原則管理



AD環境下的導入方式(2/6)

- 在「群組原則物件」節點按滑鼠右鍵→選擇「新增」
- 在「名稱」欄位→輸入群組原則物件的名稱「MicrosoftEdge」→點選「確認」



The screenshot shows the Group Policy Management console for the domain gcb.gov.tw. The left pane shows the tree structure with '群組原則物件' (Group Policy Objects) selected. A context menu is open over this folder, with '新增(N)' (New) selected. A dialog box titled '新增 GPO' (New GPO) is displayed, with 'MicrosoftEdge' entered in the '名稱(N):' (Name) field. The '確定' (OK) button is highlighted.

請點選並按右鍵

1 2 3 4

名稱	GPO 狀態	WMI 篩選器	修改日期	播
Default Domain Con...	已啟用	無	2019/10/6 下...	D
Default Domain Poli...	已啟用	無	2019/10/6 下...	D

新增 GPO

名稱(N): MicrosoftEdge

來源入門 GPO(S): (無)

確定 取消

建立一個沒有連結的 GPO

AD環境下的導入方式(3/6)

- 點選新建的群組原則物件「MicrosoftEdge」按滑鼠右鍵→選擇「匯入設定值」
- 在歡迎使用【匯入設定精靈】頁面→點選「下一步」



請點選並按右鍵

1

2

3

MicrosoftEdge

領域 詳細資料 設定 委

連結

在這個位置顯示連結(L):

下列站台、網域及組織單位已

位置

歡迎使用 (匯入設定精靈)

您可以從任何 GPO 備份將設定匯入這個群組原則物件 (GPO)。匯入設定不會修改其他 GPO 屬性，例如安全性標權、委派、連結及 WMI 篩選器連結。

注意: 如果您的網路連線不太穩定, 則執行這項操作的方法應該是, 從您備取做為群組原則管理操作之用的特定網域控制站上, 執行本機群組原則管理。

請按 [下一步] 繼續。

3 下一步(N) > 取消 說明

將設定匯入這個 GPO

AD環境下的導入方式(4/6)

- 在備份GPO頁面→點選「下一步」
- 在備份位置頁面，點選「瀏覽」→選擇欲匯入的GPO資料夾，點選「確認」→點選「下一步」
- 在來源GPO頁面→選取欲匯入的GPO→點選「下一步」



請點選 GPO 檔案位置

1 下一步(N) >

2 瀏覽(B)...

3

4 確定

5 < 上一步(B) 下一步(N) >

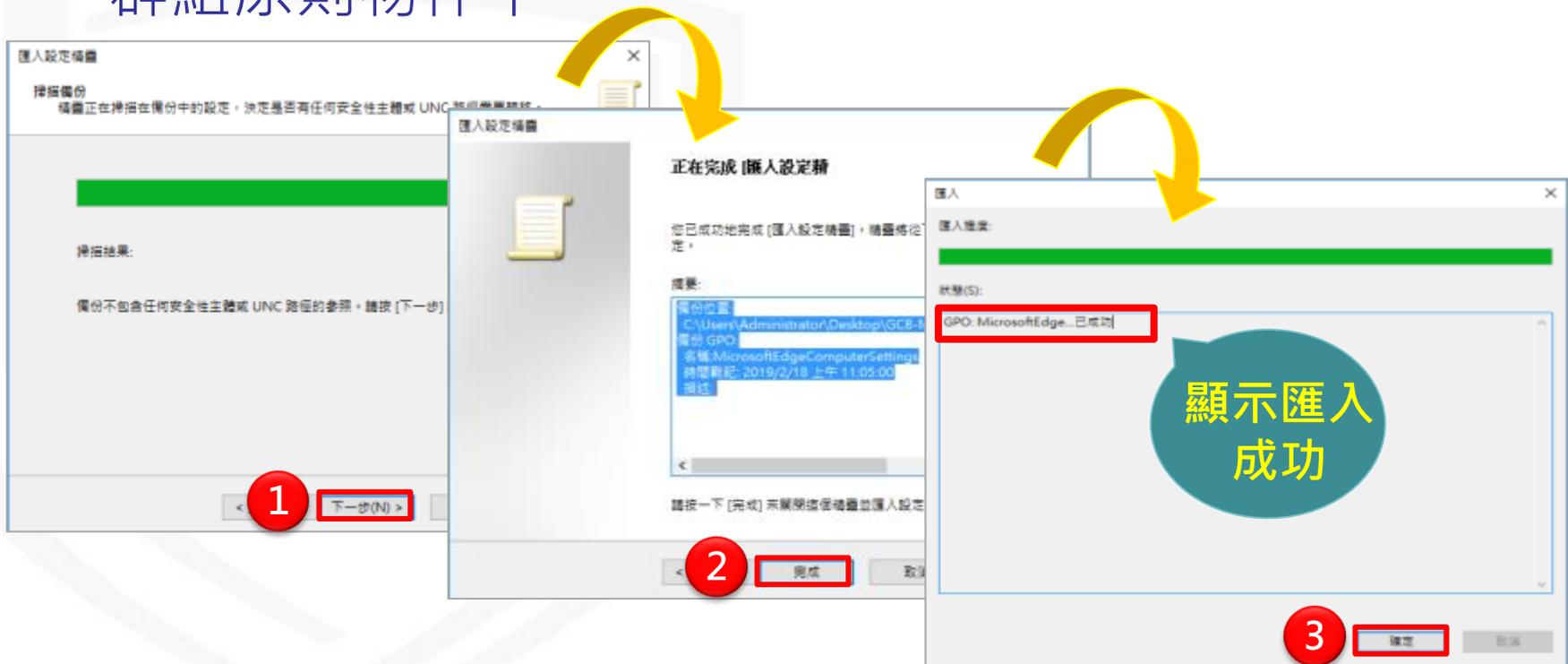
6 下一步(N) >

已備份的 GPO(A):

名稱	時間戳記	描述	網域
MicrosoftEdgeComputerSettings	2019/2/18 上午 11:...		GCB.GOV.TW

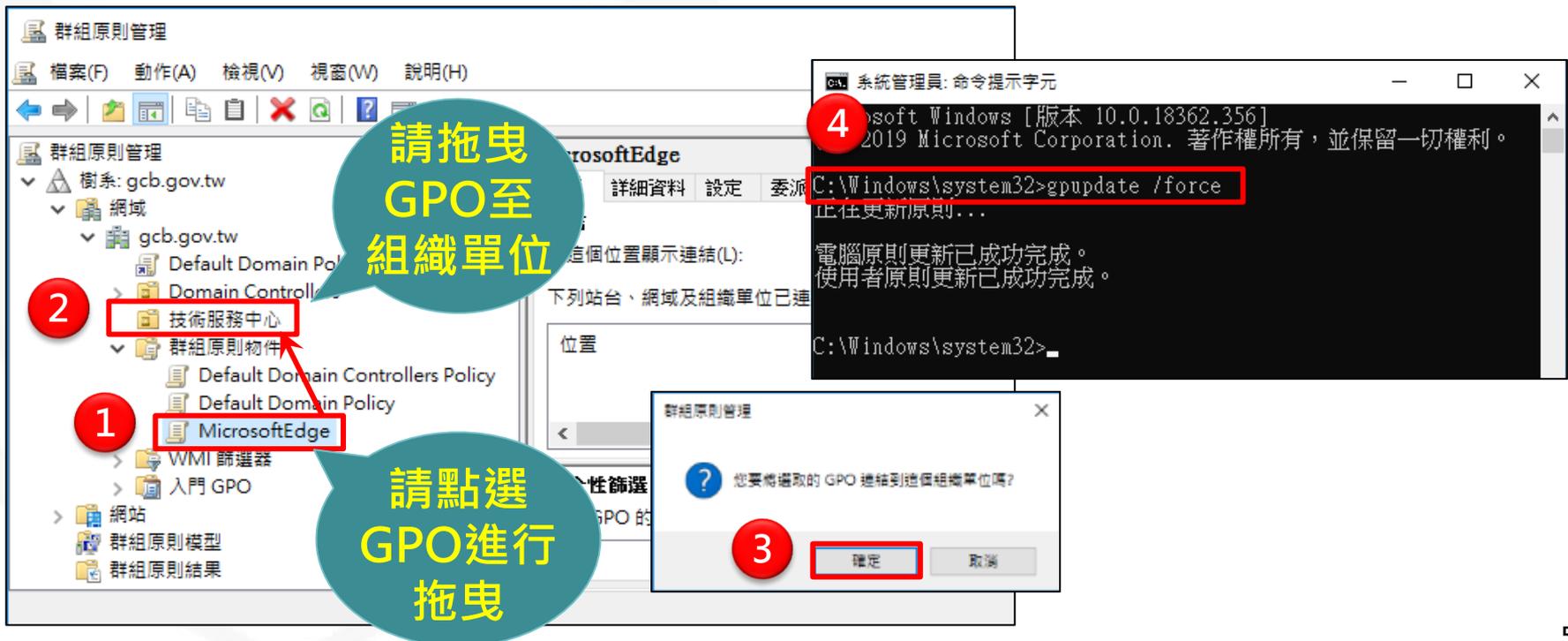
AD環境下的導入方式(5/6)

- 在掃描備份頁面→點選「下一步」
- 在正在完成匯入設定頁面→點選「完成」
- 在匯入進度的頁面→點選「確定」，完成匯入GPO至群組原則物件中



AD環境下的導入方式(6/6)

- 將新建的群組原則物件「MicrosoftEdge」拖曳至組織單位(OU) → 點選「確定」按鈕，完成部署作業
- 使用者電腦重新開機或使用gpupdate /force指令更新組態，即可更新套用的GCB設定



The screenshot illustrates the process of deploying a Group Policy Object (GPO) in an Active Directory environment. It shows the Group Policy Management console with the 'MicrosoftEdge' GPO selected and dragged to the '技術服務中心' (Technical Service Center) organizational unit. A dialog box prompts for confirmation to link the GPO to the selected OU. Simultaneously, a Command Prompt window shows the execution of the command `C:\Windows\system32>gpupdate /force`, which successfully updates the system and user policies.

1 請點選 GPO 進行拖曳

2 請拖曳 GPO 至組織單位

3 確定

4 `C:\Windows\system32>gpupdate /force`

正在更新原則...

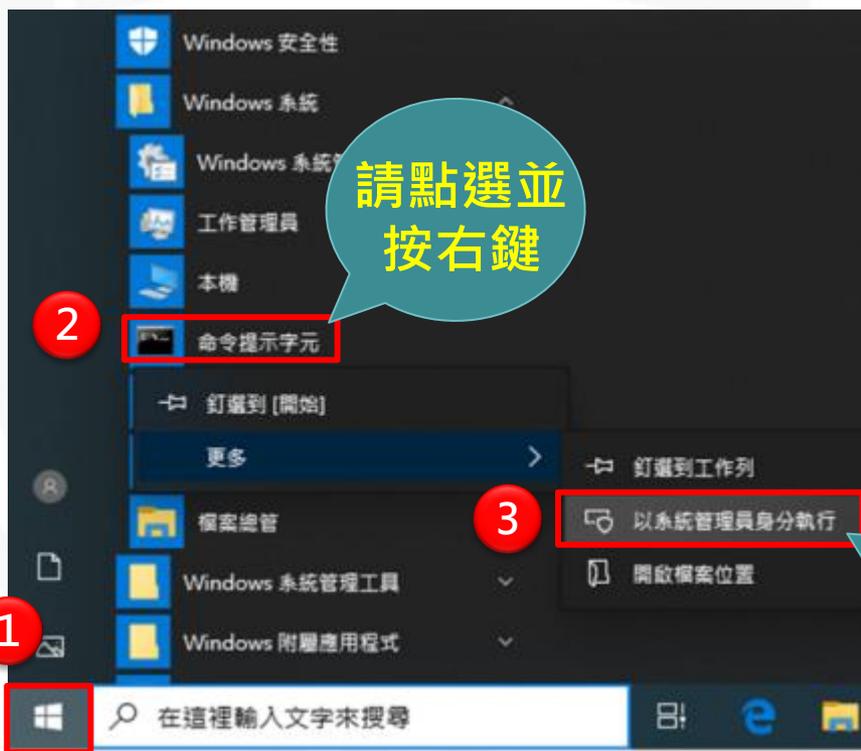
電腦原則更新已成功完成。
使用者原則更新已成功完成。

AD環境下的檢查方式(1/4)

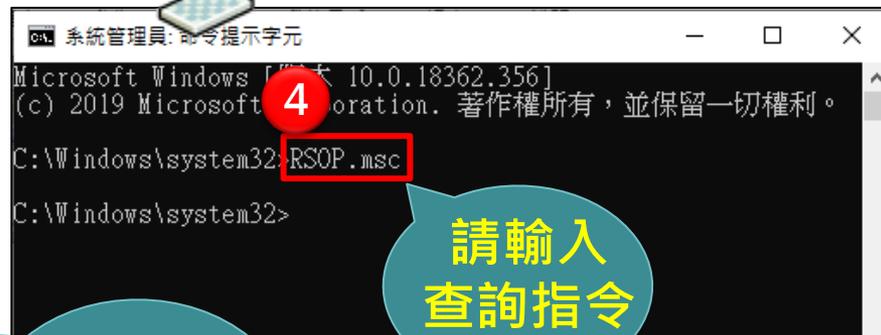
- 使用RSOP檢查群組原則

– 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→點選「以系統管理員身分執行」

– 於「命令提示字元」輸入rsop.msc查詢群組原則結果



請在網域下的使用者電腦執行檢查語法



請點選以系統管理員身分執行

AD環境下的檢查方式(2/4)

- 使用RSOP檢查群組原則，顯示如下

正在處理原則結果組...

這個 Microsoft Management Console 包含下列定義的 RSoP 嵌入式管理單元。

從 Microsoft Windows Vista Service Pack 1 (SP1) 開始，原則結果組 (RSoP) 報告不會再顯示所有 Microsoft 群組原則設定。若要檢視針對電腦或使用者套用的完整 Microsoft 群組原則設定，請使用命令列工具 gpresult。

正在處理，請稍候

選擇項目 設定
模式 記錄
使用者名稱 GCB\student
顯示使用者原則設定值 是
電腦名稱
顯示電腦原則設定值

進度:

顯示群組原則套用結果

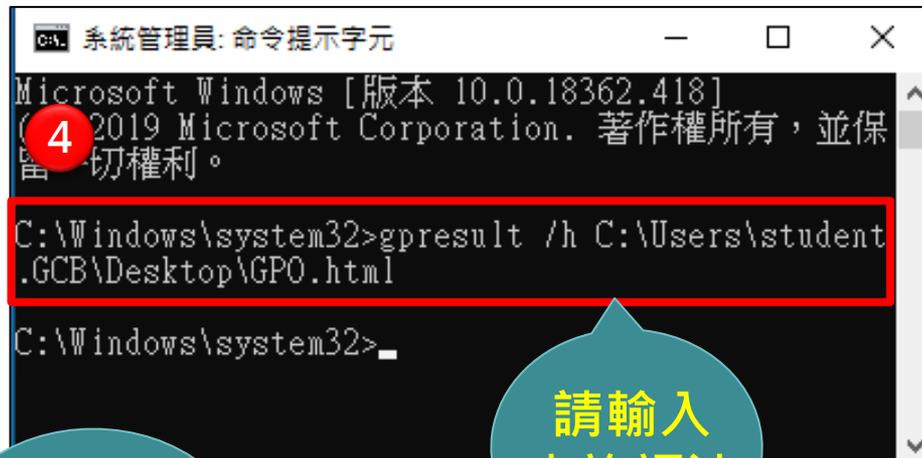
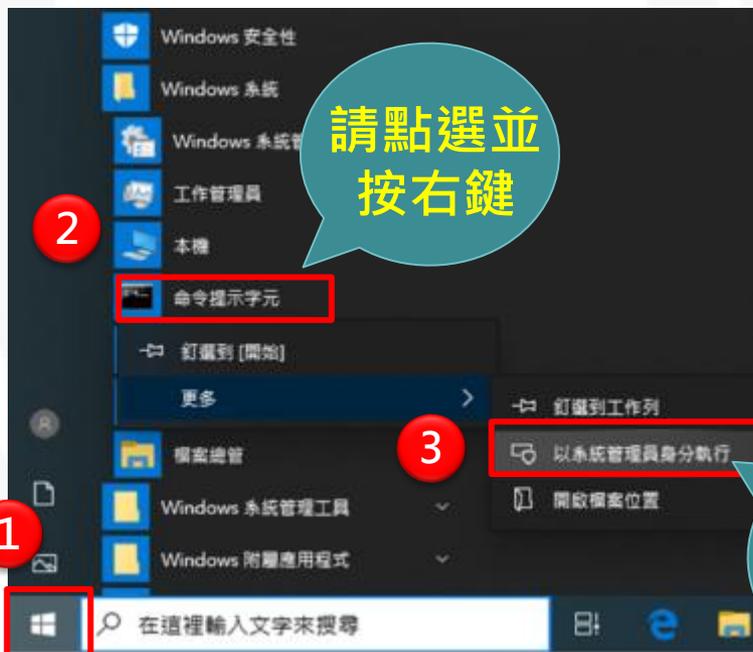
設定	狀態	GPO 名稱
<input type="checkbox"/> 設定自動填寫	已停用	MicrosoftEdge
<input type="checkbox"/> 設定「不要追蹤」	已啟用	MicrosoftEdge
<input type="checkbox"/> 允許延伸模組	已停用	MicrosoftEdge
<input type="checkbox"/> 允許 InPrivate 瀏覽	已停用	MicrosoftEdge
<input type="checkbox"/> 設定密碼管理員	已停用	MicrosoftEdge
<input type="checkbox"/> 設定快顯封鎖程式	已啟用	MicrosoftEdge
<input type="checkbox"/> 設定 Windows Defender SmartScreen	已啟用	MicrosoftEdge
<input type="checkbox"/> 設定 Cookie	已啟用	MicrosoftEdge
<input type="checkbox"/> 防止為 WebRTC 使用 Localhost IP 位址	已啟用	MicrosoftEdge
<input type="checkbox"/> 防止在 Microsoft Edge 中存取 about:flags 頁面	已啟用	MicrosoftEdge
<input type="checkbox"/> 防止略過網站的 Windows Defender SmartScreen 提示	已啟用	MicrosoftEdge
<input type="checkbox"/> 防止略過檔案的 Windows Defender SmartScreen 提示	已啟用	MicrosoftEdge

AD環境下的檢查方式(3/4)

- 使用gpresult檢查群組原則

- 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→點選「以系統管理員身分執行」

- 於「命令提示字元」輸入gpresult /h <檔案儲存路徑>\檔名.html



請點選以系統管理員身分執行

請輸入查詢語法

AD環境下的檢查方式(4/4)

- 使用gpresult檢查群組原則，顯示如下

1



GPO.html

2

顯示群組原則套用結果

群組原則結果			
GCB\DESKTOP-WIN10 的 GCB\student			
資料收集: 2019/10/13 下午 04:46:23			
全部顯示			
摘要			
顯示			
電腦詳細資料			
隱藏			
一般			
顯示			
元件狀態			
顯示			
設定			
隱藏			
原則			
隱藏			
系統管理範本			
隱藏			
已從本機電腦抓取原則定義 (ADMX 檔案)。			
Windows 元件/Microsoft Edge			
隱藏			
原則	設定	優勢 GPO	
允許 InPrivate 瀏覽	已停用	MicrosoftEdge	
允許延伸模組	已停用	MicrosoftEdge	
防止在 Microsoft Edge 中存取 about:flags 頁面	已啟用	MicrosoftEdge	
防止為 WebRTC 使用 Localhost IP 位址	已啟用	MicrosoftEdge	
防止略過檔案的 Windows Defender SmartScreen 提示	已啟用	MicrosoftEdge	
設定 Cookie	已啟用	MicrosoftEdge	
設定 Cookie		只封鎖第三方 Cookie	

AD環境下恢復原始設定方式

- 在欲取消連結的GPO上按滑鼠**右鍵**→點選「刪除」，即可將群組原則物件自組織單位(OU)中移除
- 使用者重新開機或使用gpupdate /force指令更新組態，即可恢復原始設定

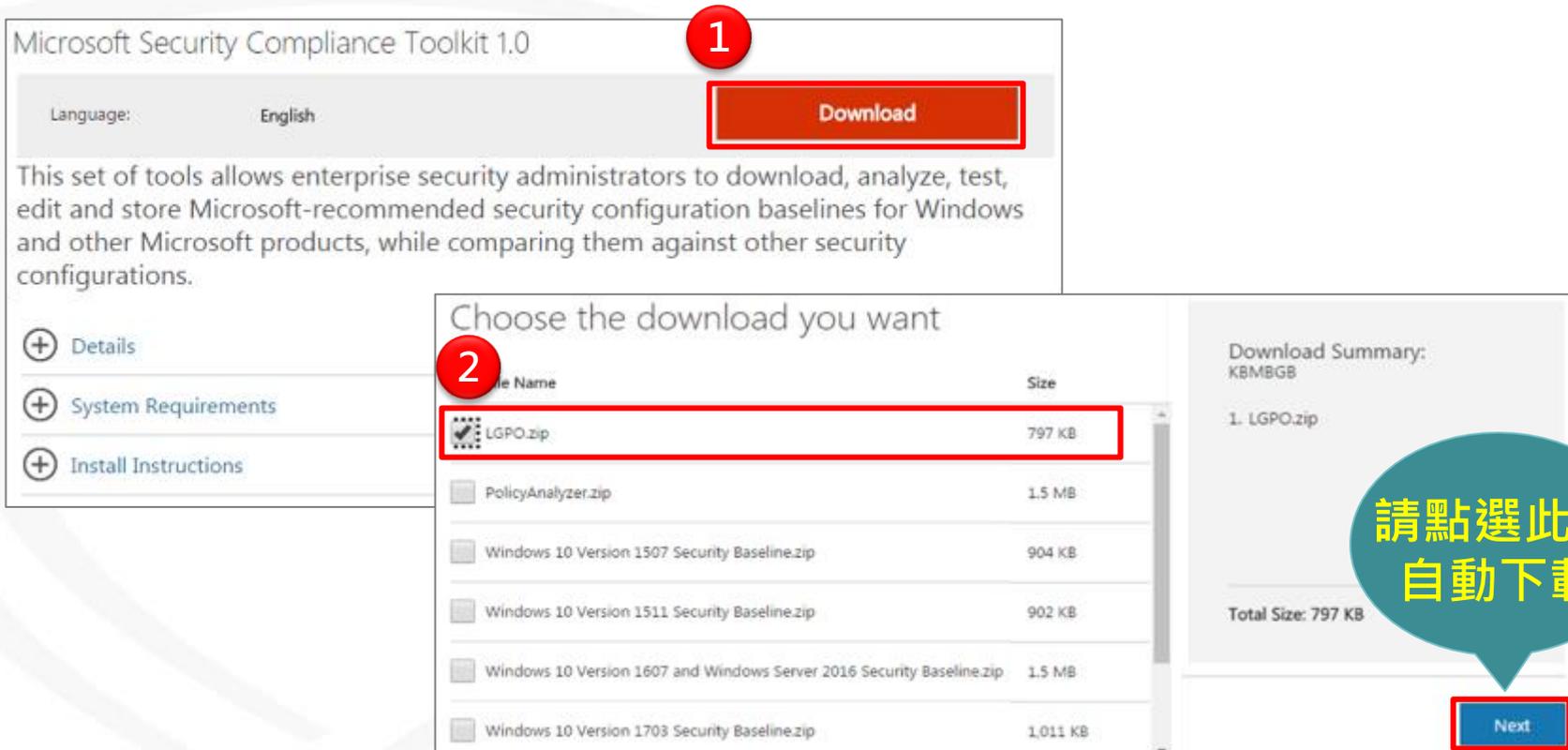


單機環境部署說明

NCCST

單機環境下的導入方式(1/4)

- 下載並解壓縮LGPO程式至電腦當中
- 下載網址：<https://www.microsoft.com/en-us/download/details.aspx?id=55319>



Microsoft Security Compliance Toolkit 1.0

Language: English **1** [Download](#)

This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

+ Details
+ System Requirements
+ Install Instructions

2 Choose the download you want

File Name	Size
<input checked="" type="checkbox"/> LGPO.zip	797 KB
<input type="checkbox"/> PolicyAnalyzer.zip	1.5 MB
<input type="checkbox"/> Windows 10 Version 1507 Security Baseline.zip	904 KB
<input type="checkbox"/> Windows 10 Version 1511 Security Baseline.zip	902 KB
<input type="checkbox"/> Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB
<input type="checkbox"/> Windows 10 Version 1703 Security Baseline.zip	1,011 KB

Download Summary:
KBMBGB

1. LGPO.zip

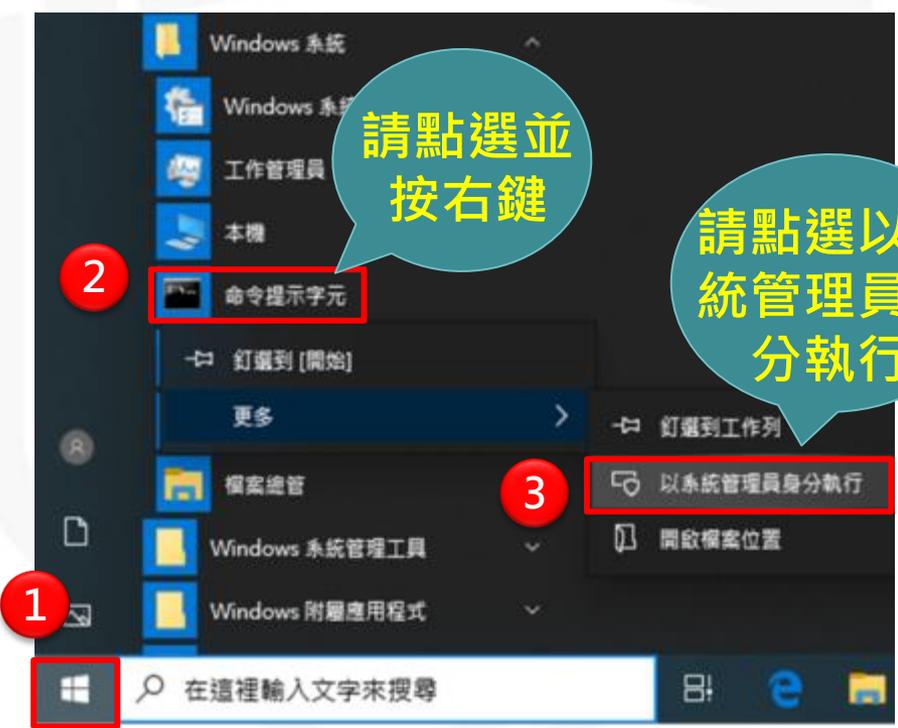
Total Size: 797 KB

[Next](#)

請點選此處
自動下載

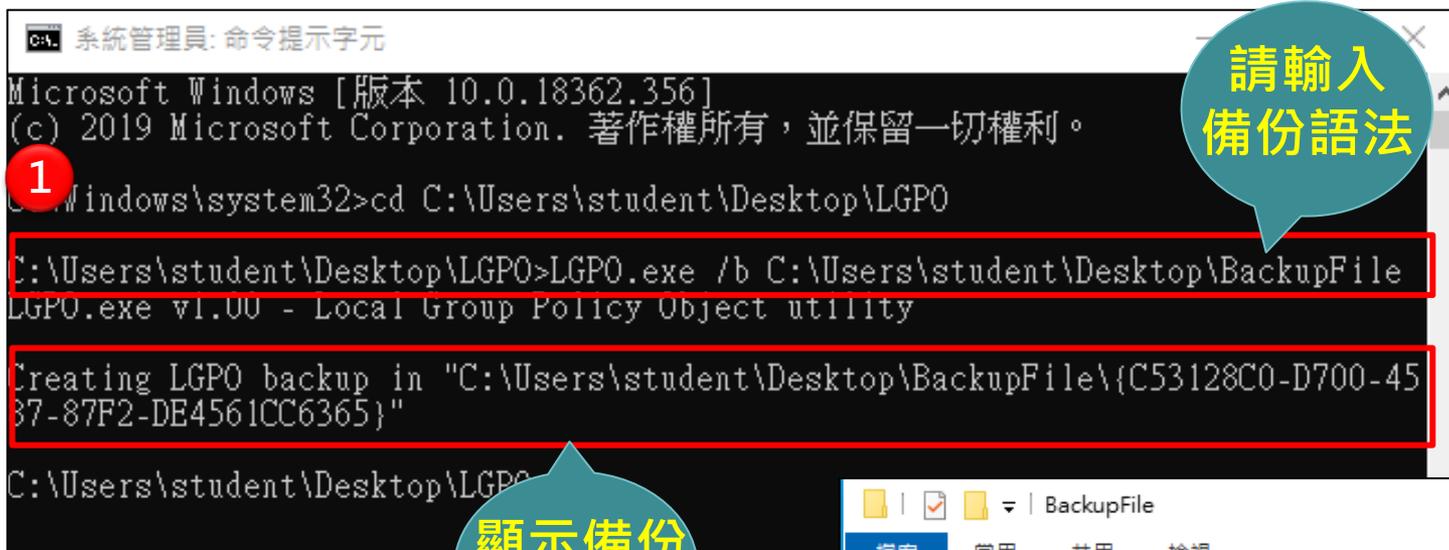
單機環境下的導入方式(2/4)

- 點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→選擇「**以系統管理員身分執行**」
- 於「命令提示字元」輸入語法**切換至LGPO目錄**
–**cd <放置LGPO解壓縮後的完整目錄路徑>**



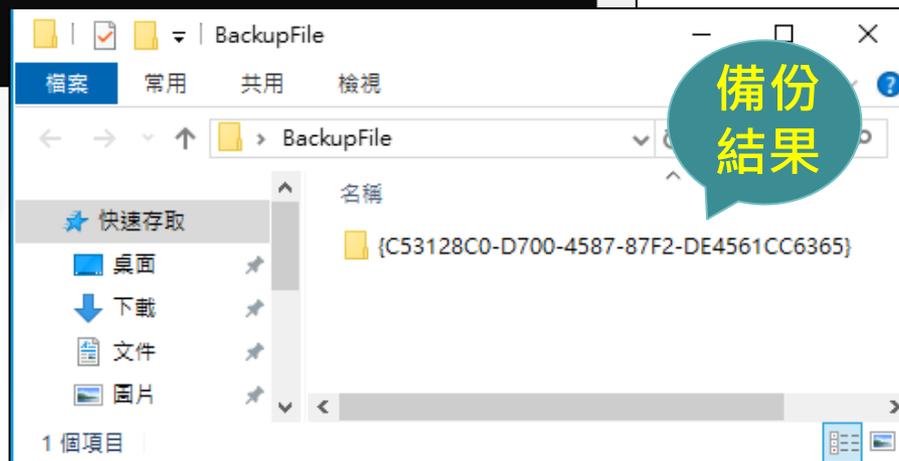
單機環境下的導入方式(3/4)

- 於「命令提示字元」輸入語法，備份電腦組態設定
–LGPO.exe /b <絕對路徑>



```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32>cd C:\Users\student\Desktop\LGPO
C:\Users\student\Desktop\LGPO>LGPO.exe /b C:\Users\student\Desktop\BackupFile
LGPO.exe v1.00 - Local Group Policy Object utility
Creating LGPO backup in "C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}"
C:\Users\student\Desktop\LGPO>
```

請輸入備份語法



顯示備份結果

單機環境下的導入方式(4/4)

- 於「命令提示字元」輸入語法，匯入Microsoft Edge GPO組態設定
 - LGPO.exe /g <絕對路徑>
- 重新開機或使用gpupdate /force指令更新組態，即可更新套用的GPO設定

The screenshot illustrates the process of importing and updating a GPO in a single-machine environment. It is divided into four numbered steps:

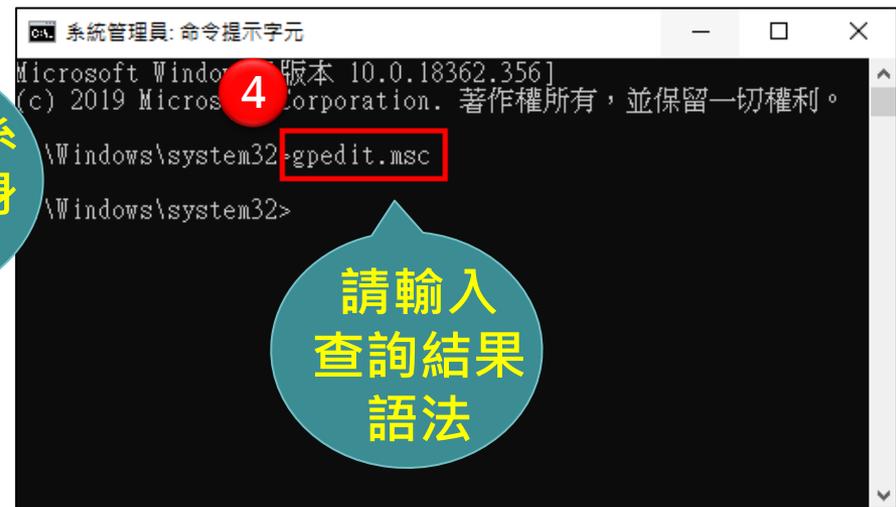
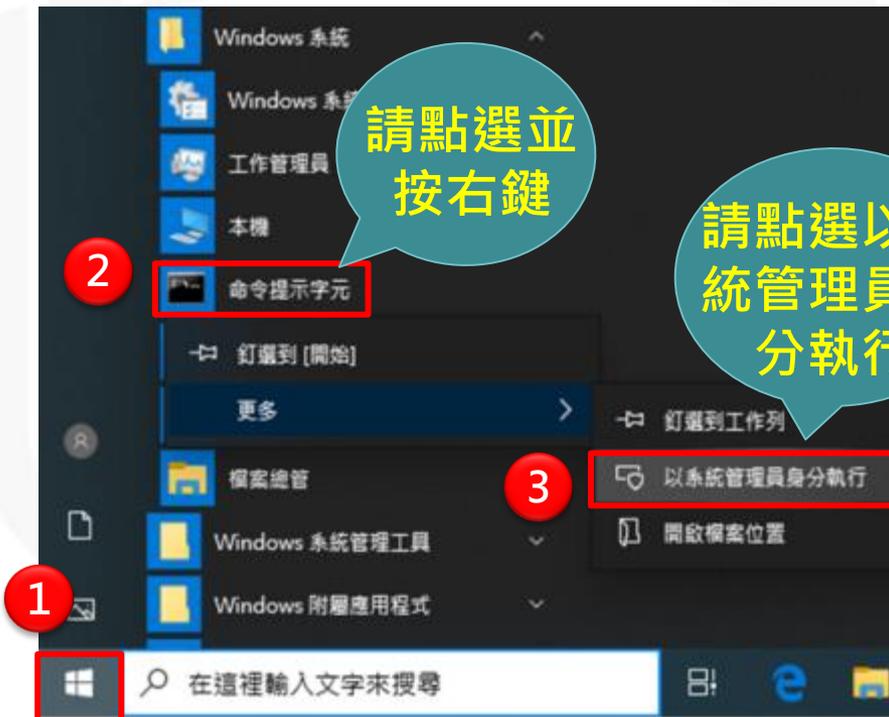
- 1**: In the File Explorer, the path `sktop\GCB-MicrosoftEdge-gpos\MicrosoftEdgeComputerSettings\{81B28E64-9352-49E6-B2FD-5698145FB76B}` is highlighted. A callout bubble says: **請複製 GPO 完整路徑** (Please copy the full GPO path).
- 2**: The Command Prompt shows the command `cd C:\Users\student\Desktop\LGPO` and the execution of `LGPO.exe /g C:\Users\student\Desktop\GCB-MicrosoftEdge-gpos\MicrosoftEdgeComputerSettings\{81B28E64-9352-49E6-B2FD-5698145FB76B}`. A callout bubble says: **請輸入 匯入語法** (Please enter the import syntax).
- 3**: The Command Prompt shows the command `Import Machine settings from registry.pol: C:\Users\student\Desktop\GCB-MicrosoftEdge-gpos\MicrosoftEdgeComputerSettings\{81B28E64-9352-49E6-B2FD-5698145FB76B}\DomainSysvol\GPO\Machine\registry.pol`. A callout bubble says: **更新組態** (Update configuration).
- 4**: The Command Prompt shows the command `gpupdate /force` and the output: `正在更新原則...` (Updating policies...). A callout bubble says: **顯示匯入結果** (Display import results).

單機環境下的檢查方式(1/2)

- 使用gpedit.msc檢查群組原則

- 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→選擇「以系統管理員身分執行」

- 於「命令提示字元」輸入gpedit.msc



單機環境下的檢查方式(2/2)

- 使用gpedit.msc檢查群組原則，顯示如下

設定	狀態	註解
設定自動填寫	已停用	否
允許延伸模組	已停用	否
允許 InPrivate 瀏覽	已停用	否
設定密碼管理員	已停用	否
設定「不要追蹤」	已啟用	否
設定快顯封鎖程式	已啟用	否
設定 Windows Defender SmartScreen	已啟用	否
設定 Cookie	已啟用	否
防止為 WebRTC 使用 Localhost IP 位址	已啟用	否
防止在 Microsoft Edge 中存取 about:flags 頁面	已啟用	否
防止略過網站的 Windows Defender SmartScreen 提示	已啟用	否
防止略過檔案的 Windows Defender SmartScreen 提示	已啟用	否
允許網址列下拉菜單列出建議	尚未設定	否
允許 Microsoft 相容性清單	尚未設定	否
允許在結束時清除瀏覽資料	尚未設定	否
允許為書籍庫更新設定	尚未設定	否
允許開發人員工具	尚未設定	否

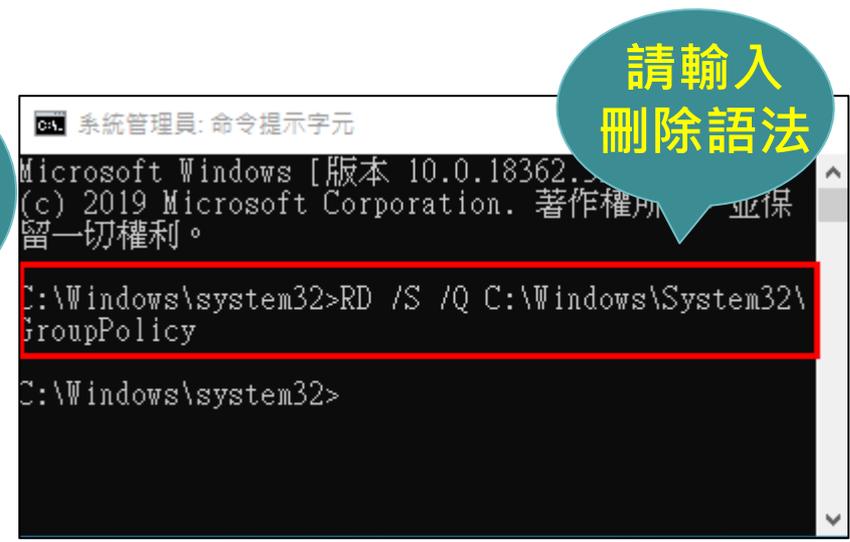
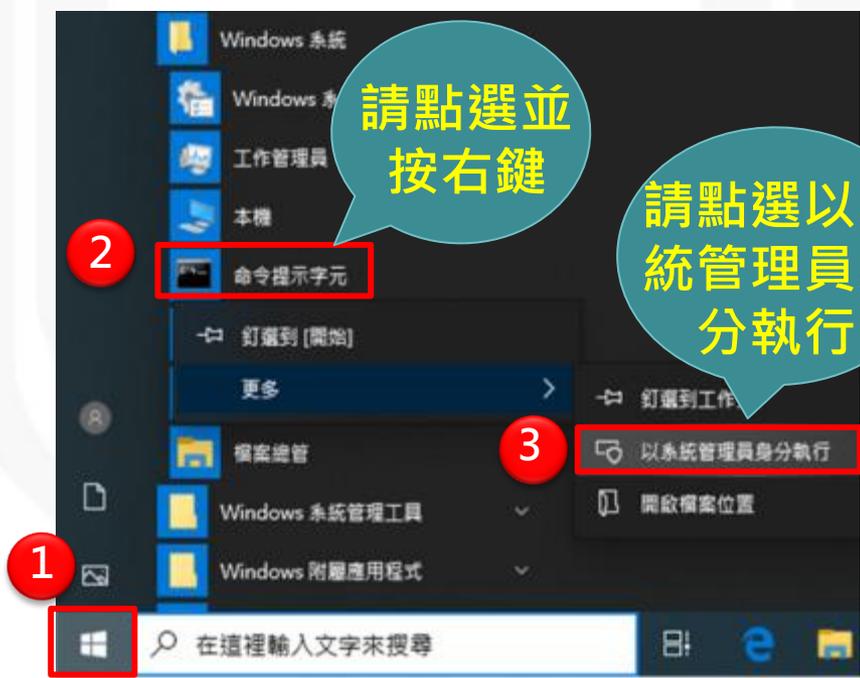
單機環境下恢復原始設定方式(1/2)



- 使用LGPO恢復原始設定

- 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→選擇「以系統管理員身分執行」

- 執行RD /S /Q C:\Windows\System32\GroupPolicy進行刪除



單機環境下恢復原始設定方式(2/2)



- 使用LGPO恢復原始設定

- 於「命令提示字元」輸入語法切換至LGPO目錄
- 執行LGPO.exe /g <絕對路徑>，匯入備份的GPO檔案
- 重新開機或使用gpupdate /force指令更新組態

The screenshot shows a Windows Command Prompt window with the following text:

```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32> cd C:\Users\student\Desktop\LGPO
C:\Users\student\Desktop\LGPO> LGPO.exe /g C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}
LGPO.exe v1.00 - Local Group Policy Object utility

Created directory for audit policy
Copied C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
to C:\Windows\system32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv
Clearing existing audit policy
Apply Audit policy from C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}\DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}\DomainSysvol\GPO\User\registry.pol

C:\Users\student\Desktop\LGPO> gpupdate /force
正在更新原則...
電腦原則更新已成功完成。
使用者原則更新已成功完成。

C:\Users\student\Desktop\LGPO>
```

Callouts in the image:

- 1: Points to the directory change command: `cd C:\Users\student\Desktop\LGPO`
- 2: Points to the LGPO command: `LGPO.exe /g C:\Users\student\Desktop\BackupFile\{C53128C0-D700-4587-87F2-DE4561CC6365}`
- 3: Points to the update command: `gpupdate /force`

Text bubbles:

- 請切換目錄 (Please switch directory)
- 請輸入匯入語法 (Please enter import syntax)
- 更新組態設定 (Update configuration)

實作練習

A large, faint watermark of the NCCST logo is centered on the page. It features a shield shape with the acronym "NCCST" in a light gray font inside.

實作練習-環境說明

環境說明

- 本次採用單機環境進行實作練習
- 單機部署環境說明
 - VM名稱：5.Microsoft Edge
 - 本機帳號：Student；密碼：1qaz@WSX3edc
- VM環境皆已安裝實作練習所需之LGPO與LocalGPO軟體，並於桌面放置Microsoft Edge GPO檔與指令文字檔

實作練習1



實作說明

- 請使用LGPO部署Microsoft Edge GPO
 - 步驟1：於「命令提示字元」按滑鼠右鍵，選擇「以系統管理員身分執行」
 - 步驟2：於「命令提示字元」輸入切換至LGPO目錄語法
 - 步驟3：於「命令提示字元」輸入備份電腦組態設定語法LGPO.exe /b <絕對路徑>
 - 步驟4：於「命令提示字元」輸入匯入GPO組態設定語法LGPO.exe /g <絕對路徑>
 - 步驟5：於「命令提示字元」輸入更新組態設定語法gpupdate /force

實作練習2(1/2)

實作說明

- 驗證「防止略過網站的Windows Defender SmartScreen提示」設定
 - 步驟1：請使用Edge開啟測試網址
<https://nav.smartscreen.msft.net/>
 - 步驟2：點選網頁中的URL Rep Demos畫面測試
 - 步驟3：檢視套用GPO狀況下，是否可防止使用者略過警示繼續存取網站

URL Rep Demos

Is This Phishing?



Alert the user to a suspicious page and ask for feedback

Phishing Page



A page known for phishing that should be blocked

Malware Page



A page that hosts malware and should be blocked

點選
測試

已報告此網站為不安全
已託管 nav.smartscreen.msft.net

我們建議您不要繼續瀏覽此網站。已有使用者向 Microsoft 回報此網站包含會對電腦造成風險的威脅，此威脅可能會造成個人或財務資訊洩漏。

其他資訊

已有使用者報告此網站包含下列威脅：

- 網路釣魚威脅：這是一個網路釣魚網站，旨在誘使您提供個人或財務資訊。

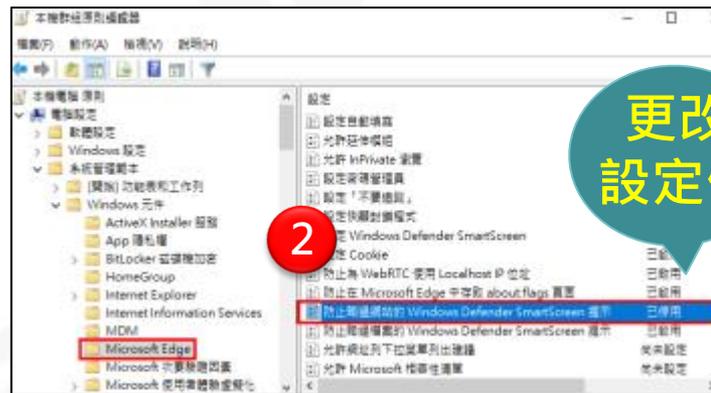
Windows Defender SmartScreen

設定
啟用

實作練習2(2/2)

實作說明

- 比對當「防止略過網站的Windows Defender SmartScreen提示」設定為「停用」之差異
 - 步驟1：於「命令提示字元」按滑鼠右鍵，選擇「以系統管理員身分執行」，輸入gpedit.msc
 - 步驟2：更改本項群組原則設定值為「停用」
 - 步驟3：關閉Edge瀏覽器，重新使用Edge開啟測試網址 <https://nav.smartscreen.msft.net/>
 - 步驟4：點選網頁中的URL Rep Demos畫面測試
 - 步驟5：檢視停用狀況下，是否可防止使用者略過警示繼續存取網站



實作練習3(1/2)

實作
說明

- 驗證「設定快顯封鎖程式」設定
 - 步驟1：請使用Edge開啟測試網址
<http://www.popupstest.com/popupstest1.html>
 - 步驟2：檢視快顯示窗是否被阻擋

PopupTest 1

This page will launch a total of 10 popup windows

Loading Popup windows...



Done!

If you didn't see any popup windows,
you are probably using a popup blocker
and it is working.

Or, you are using a non-standard browser...
Or, you have Java turned off...

BACK

PopupTest 1

This page will launch a total of 10 popup windows

Loading Popup windows.



Done!

If you didn't see any popup windows,
you are probably using a popup blocker
and it is working.

Or, you are using a non-standard browser...
Or, you have Java turned off...

BACK

允許 'http://www.popupstest.com/popup1.html'
允許 'http://www.popupstest.com/popup2.html'
允許 'http://www.popupstest.com/popup3.html'
允許 'http://www.popupstest.com/popup4.html'
允許 'http://www.popupstest.com/popup5.html'
允許 'http://www.popupstest.com/popup6.html'
允許所有快顯

Microsoft Edge 已封鎖來自 www.popupstest.com 的快
顯。

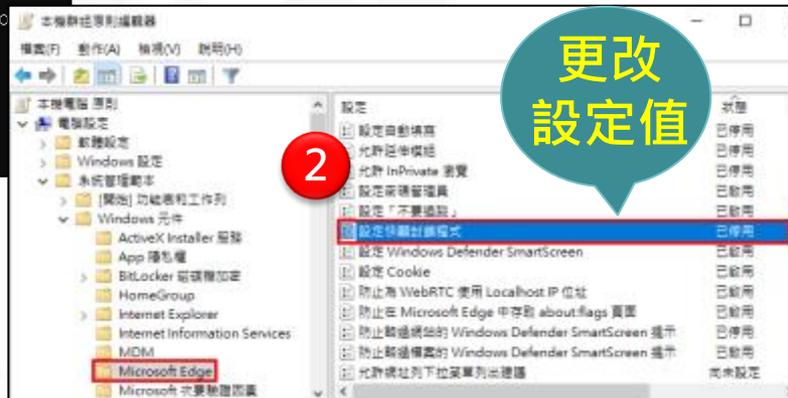
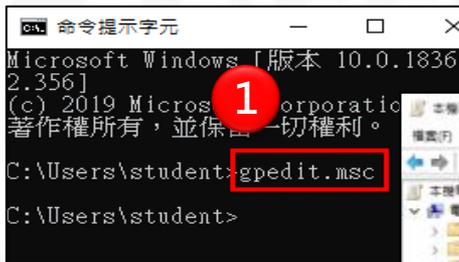
允許一次 ^

一律允許

實作練習3(2/2)

實作說明

- 比對「設定快顯封鎖程式」設定「停用」之差異
 - 步驟1：於「命令提示字元」輸入gpedit.msc
 - 步驟2：更改本項群組原則設定值為「停用」
 - 步驟3：關閉Edge瀏覽器，重新使用Edge開啟測試網址
<http://www.popuptest.com/popuptest1.html>
 - 步驟4：檢視停用狀況下，是否可封鎖快顯程式



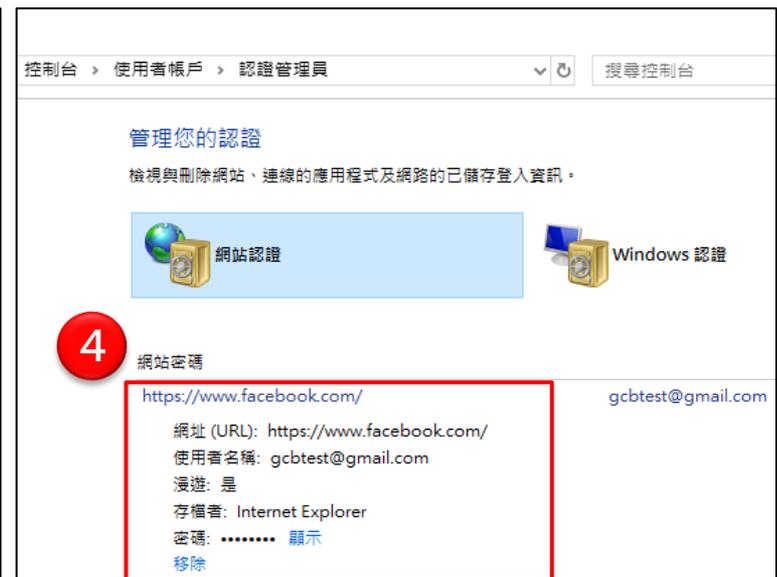
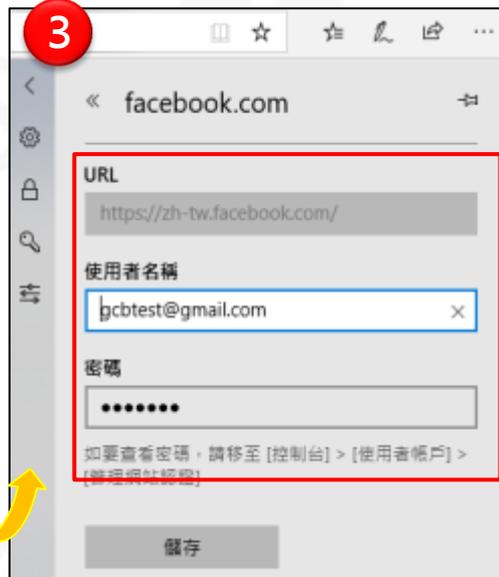
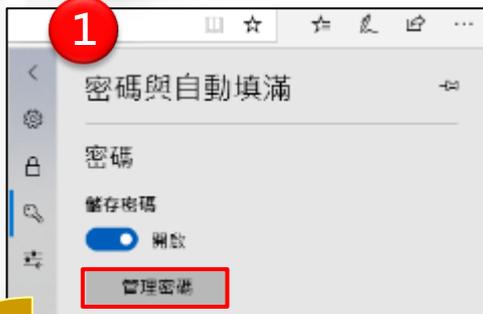
實作練習4

實作
說明

- 驗證「設定密碼管理員」設定

– 步驟1：請開啟Edge→點選「設定」→點選「密碼與自動填滿」，檢視儲存密碼功能是否關閉以及已儲存的資訊是否可以異動

– 步驟2：點擊開始→搜尋「認證管理員」，檢視是否可以看到帳號密碼



實作練習5(1/2)

實作
說明

- 驗證「設定自動填寫」設定

– 步驟1：請使用Edge開啟測試網址

<https://anttiviljami.github.io/browser-autofill-phishing/>

– 步驟2：點選Name的輸入欄位2下，點選自動填寫功能帶出之資訊，按下「Submit」

– 步驟3：將網頁的address資訊進行編碼轉換，轉換網址<https://www.ifreesite.com/unicode-ascii-ansi.htm>

請在欄位
內點2下



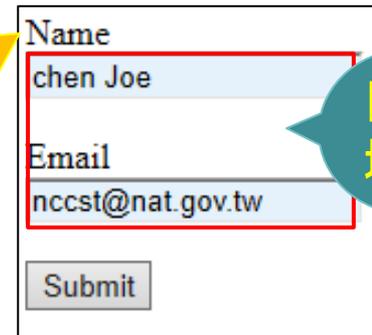
Name
Your Name

chen Joe
nccst@nat.gov.tw

管理表單

This screenshot shows a web form with a 'Name' field. The input field contains 'Your Name' and is highlighted with a red box. A dropdown menu is open below it, showing suggestions: 'chen Joe' and 'nccst@nat.gov.tw'. A yellow arrow points from the input field to the dropdown menu.

點選
資訊



Name
chen Joe

Email
nccst@nat.gov.tw

Submit

This screenshot shows the same web form after the autofill function has been used. The 'Name' field now contains 'chen Joe' and the 'Email' field contains 'nccst@nat.gov.tw'. Both fields are highlighted with red boxes. A 'Submit' button is visible at the bottom.

自動
填入

實作練習5(2/2)

實作說明

- 驗證「設定自動填寫」設定

– 步驟4：檢視轉換後之資訊是否與Edge瀏覽器的「密碼與自動填滿」儲存資訊一致



The screenshot shows a browser window with the URL `https://httpbin.org/post`. The response is a JSON object with a `form` field. The `address` field contains the value `"\u53f0\u5317\u5e02\u5927\u5b89"`, which is highlighted with a red box and labeled with a red circle '1'. A callout bubble points to this value with the text "請複製引號內文字".

Below the browser window, a character encoding conversion tool is shown. The input field contains the same Unicode string, highlighted with a red box and labeled with a red circle '2'. A callout bubble points to the input with the text "顯示結果". The tool has two buttons: "字元轉換為Unicode" and "Unicode轉換為字元". The output field shows the converted string `"\u53f0\u5317\u5e02\u5927\u5b89\u5340\u5bcc\u967d\u8857116\u865f"`, highlighted with a red box and labeled with a red circle '3'. A callout bubble points to the output with the text "請貼上".

- [市面近1/4的VPN服務有漏洞，隱匿不成反而洩漏用戶IP](#)
- [2019資安預測趨勢提七大重點：資料外洩通報與網路釣魚將大增](#)
- [鎖定Edge漏洞的攻擊程式曝光](#)
- [查身分證功能防詐騙 網頁中獎廣告別上當](#)
- [Several Cryptojacking Apps Found on Microsoft Store](#)
- [小心！瀏覽器自動填入功能可能讓你儲存的個資被偷光光](#)
- [你不曉得的「按讚」情報威力](#)
- [資安業者在Microsoft Store發現8款程式暗藏挖礦功能](#)
- [Windows Defender SmartScreen 常見問題集](#)
- [維基百科Wikipedia](#)

報告完畢
敬請指教

NCCST