教育體系資安檢核 GCB 導入案例分享

臺灣大學計資中心

網路組游子興

davisyou@ntu.edu.tw

大綱

* 技服GCB 規則 Review
* 技服GCB 規則盲點
* GCB 排除項 Reviews
* GCB 導入工具
* GCB 導入方法
* GCB 套用後檢測方法
* GCB 套用前後差異

技服GCB 規則 Review

GCB 作業系統
Windows 10

* Windows10 Account Settings

2	Windows 10 Account Settings	TWGCB-01-005-0002	帳戶原則\密碼原則	密碼最長使用期限	▪ 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在 1 至 999 天之後到期；或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之間的任何數值 ▪ 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限	90 天以下	CCE-ID：CCE-4353 5-4

GCB 作業系統
Windows 10

3	Windows 10 Account Settings	TWGCB-01-005-0003	帳戶原則\密碼原則	最小密碼長度	▪此項原則設定決定使用者帳戶的密碼可包含的最少字元數。可以設定介於 1 到 14 個字元之間的值 ▪將字元數設為 0，則表示不需要密碼	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	8 個字元以上	CCE-ID：CCE-41679-2
4	Windows 10 Account Settings	TWGCB-01-005-0004	帳戶原則\密碼原則	密碼必須符合複雜性需求	▪此項原則設定決定密碼是否必須符合複雜性需求 ▪如果啟用了此原則，則密碼必須符合下列最小需求： -不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元 -長度至少為 6 個字元 -包含下列四種字元中的三種： (1)英文大寫字元(A 到 Z) (2)英文小寫字元(a 到 z) (3)10 進位數字(0 到 9) (4)非英文字母字元(例如：!、$、	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求	啟用	CCE-ID：CCE-42872-2

GCB 作業系統
Windows 10

* 政府組態基準GCB_Microsoft Windows 10 說明文件(V1.3).docx

表1　Windows 10 組態基準項目統計

項次	項目	項數	合計
1	Windows10 Account Settings	9	345
2	Windows10 Computer Settings	291	
3	Windows10 User Settings	12	
4	Windows10 Firewall Settings	33	

Windows Server 2016

表1　Windows Server 2016 組態基準項目統計

項次	項目	項數	小計	合計
1	Windows Server 2016 Account Settings	9	299	690
	Windows Server 2016 Common Settings	290		
2	Windows Server 2016 DC Server	27	27	
3	Windows Server 2016 DNS Server	119	119	
4	Windows Server 2016 File Server	124	124	
5	Windows Server 2016 Web Server	121	121	

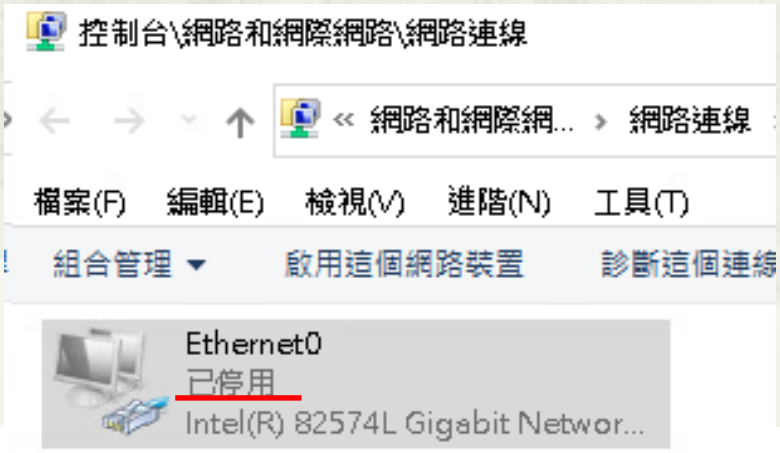
技服GCB Review

項目	技服 GCB 規則項數
Win10	345
Windows Server 2016	590
Red Hat Enterprise Linux 8	292
IE11	154
Chrome	33
Firefox	52
Edge	12
Wireless	19
Fortigate Firewall	46
…	…
總數	1500+

技服GCB Review

* 若完整導入技服GCB 所有項目
* → **突破性感染的 %** 為多少??

* 100% 有效的CCB設定其實只需要一個
* → **“停用”**網路卡



技服GCB Review

* 完全不接種(套用GCB規則0%)→ 感染率 60%
* 接種第一劑(套用GCB規則60%) → 感染率 30%
* 接種第二劑(套用GCB規則70%) → 感染率 20%
* ....
* 完整接種(套用GCB規則100%) → 感染率 5%

應建立更接地氣的 GCB 規範

- 建議技服GCB規則可增加”風險等級:高/中/低”欄位可供參考
- 應區分不同工作角色(行政人員、程式設計師、網管人員等)，訂立多套 GCB 規則範本
  - 若所有電腦不區分工作角色都套用相同規則，導致排除項非常多，可能造成資安破口。
- 取其 GCB 精神，而非規則細項
  - 可先從計中管理設備做起
    - Cisco Config Template: 套用統一設定檔範本 (Login,NTP,SSH,SNMP, ACL等)

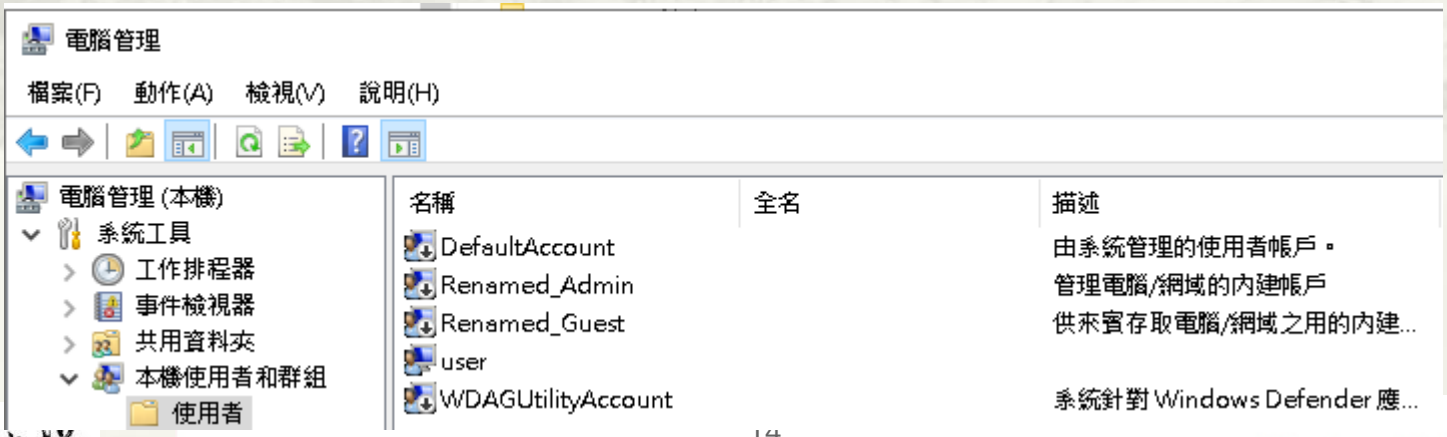
Cisco Config Template 範例

```
權限相關
  (config)# enable secret 12345
  (config)# username davis secret 12345
  password 加密
  (config)# service password-encryption

Line VTY
  ip access-list standard telnet-acl
    permit 140.112.0.0 0.0.255.255
    permit 120.96.0.0 0.0.31.255 or 120.96.0.0/19
    permit 120.96.240.0 0.0.7.255 or 120.96.240.0/21
    permit 120.96.248.0 0.0.3.255 or 120.96.248.0/22

  (config)# line vty 0 15
  (config-line)# login local
  (config-line)# access-class telnet-acl in

關閉 HTTP & HTTPS
  (config)# no ip http server
  (config)# no ip http secure-server

Logging
  (config)#no logging console
  (config)#logging buffered 96000
  (config)#service timestamps log datetime localtime show-timezone

時間相關
  (config)#clock timezone ROC 8
           clock timezone TW 8

          #clock set 10:30:00 15 Apr 2013
```

技服 GCB 規則盲點

Renamed_Admin Renamed_Guest 統一改成 Renamed_xxx 有更安全?

93	Windows 10 Computer Settings	TWG CB-01 -005-0 093	安全性選項\帳戶	帳戶：重新命名系統管理員帳戶	此項原則設定將重新命名已知的 Administrator 帳戶，透過使用不同的帳戶名稱與 Administrator 帳戶之安全性識別碼(SID)相關聯，使得未經授權的人員較不容易猜出有此特殊權限的使用者名稱與密碼組合	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名系統管理員帳戶	Renamed_Admin	CCE-ID：CCE-42970-4
94	Windows 10 Computer Settings	TWG CB-01 -005-0 094	安全性選項\帳戶	帳戶：重新命名來賓帳戶名稱	此項原則設定將重新命名已知的 Guest 帳戶，透過使用不同的帳戶名稱與 Guest 帳戶之安全性識別碼(SID)相關聯，使得未經授權的人員較不容易猜出此使用者名稱與密碼組合	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名來賓帳戶名稱	Renamed_Guest	CCE-ID：CCE-43078-5

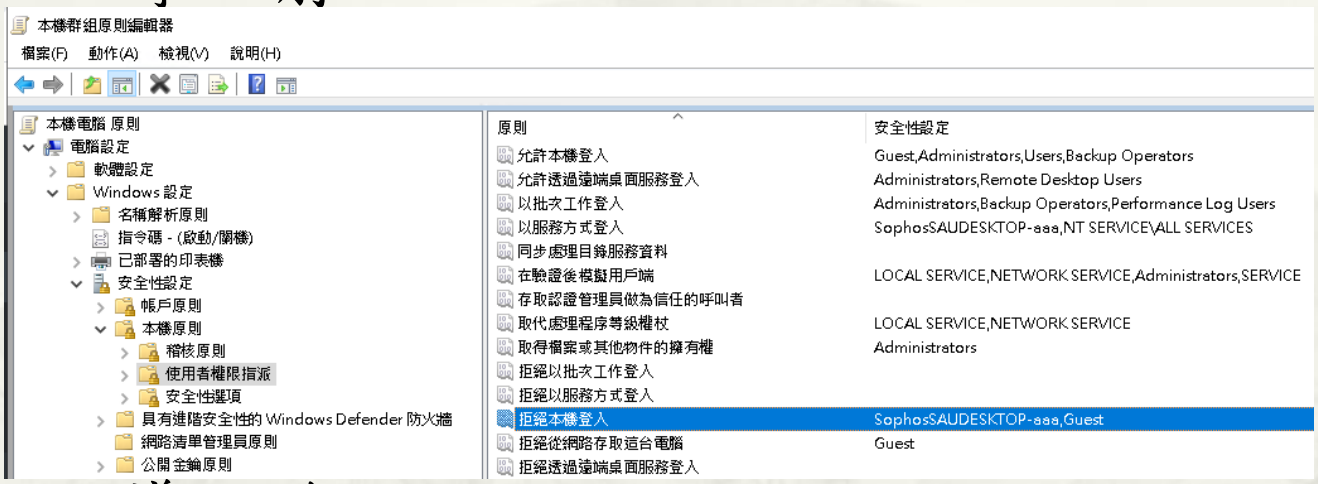


”拒絕xxx” 相關設定 Overwrite 原先設定值

192	Windows 10 Computer Settings	TWG CB-01 -005-0 192	使用者權限指派	拒絕從網路存取這台電腦	▪ 此項原則設定決定會阻止哪些使用者從網路存取電腦 ▪ 如果使用者帳戶同時受限於「拒絕從網路存取這台電腦」與「從網路存取這台電腦」這兩種原則，則此項原則設定會取代「從網路存取這台電腦」原則設定	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕從網路存取這台電腦	NT AUTHORITY\Local Account, Guests	CCE-ID：CCE-4262 1-3
193	Windows 10 Computer Settings	TWG CB-01 -005-0 193	使用者權限指派	拒絕以批次工作登入	▪ 此項原則設定決定會阻止哪些帳戶以批次工作登入 ▪ 如果使用者帳戶同時受限於「拒絕以批次工作登入」與「以批次工作登入」這兩種原則，則此項原則設定會取代「以批次工作登入」原則設定	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕以批次工作登入	Guests	CCE-ID：CCE-4342 8-2
194	Windows 10 Computer Settings	TWG CB-01 -005-0 194	使用者權限指派	拒絕以服務方式登入	▪ 此項原則設定決定會阻止哪些服務帳戶以服務方式登錄處理程序 ▪ 如果帳戶同時受限於「拒絕以服務方式登入」與「以服務方式登	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒	Guests	CCE-ID：CCE-4417 2-5
195	Windows 10 Computer Settings	TWG CB-01 -005-0 195	使用者權限指派	拒絕本機登入	▪ 此項原則設定決定將阻止哪些使用者登入電腦 ▪ 如果帳戶同時受限於「拒絕本機登入」與「允許本機登入」這兩種原則，則此項原則設定會取代「允許本機登入」原則設定	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕本機登入	Guests	CCE-ID：CCE-4385 4-9

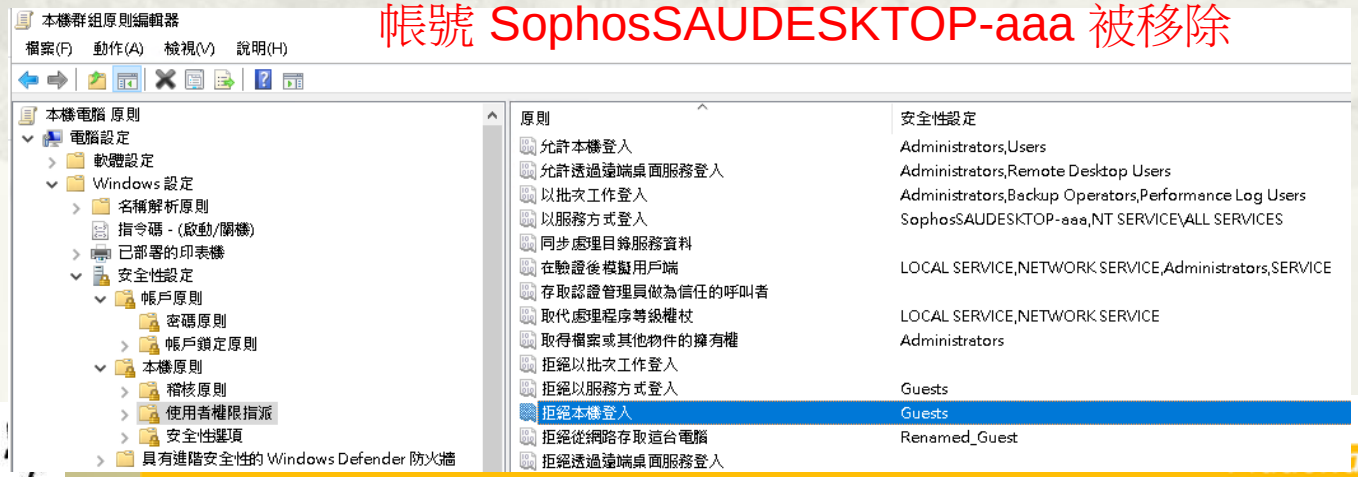
”拒絕xxx”相關設定 Overwrite 原先設定值

* GCB 導入前



* GCB 導入後

帳號 SophosSAUDESKTOP-aaa 被移除



GCB 排除項 Review

GCB 排除項

項目	技服 GCB 規則項數	排除項: NCTU + NTU	排除比率
Win10	345	56	16%
IE11	154	34	22%
Chrome	33	11 +4	45%
Firefox	52	0 + 3	6%
Edge	12	0	0%

GCB 排除項來源

- 顯而易見、難以達成之技服 GCB 規則
- 技服 GCB 網站FAQ
- 其他學校經驗 (智慧財產權)
- 自行測試及使用者回饋

顯而易見、難以達成
技服 GCB 規則

* 瀏覽器 Chrome

6	Google Chrome Computer Settings	TWGCB-02-003-0006	Google Chrome	Google Chrome	封鎖第三方 Cookie	▪啟用這項設定即可禁止非瀏覽器網址列網域的網頁元素所設定的 Cookie ▪停用這項設定可允許非瀏覽器網址列網域的網頁元素所設定的 Cookie，並且禁止使用者變更這項設定 ▪如果未設定這項政策，系統會啟用第三方 Cookie，不過使用者可以加以變更	電腦設定\系統管理範本\Google Chrome\封鎖第三方 Cookie	啟用	

顯而易見、難以達成
技服 GCB 規則

* 無線網路

項次	TWGCB-ID	類別	原則設定名稱	說明	D-Link 設定路徑	EDIMAX 設定路徑	ZyXEL 設定路徑
5	TWGCB-03-001-0005		變更預設 SSID	變更預設的 SSID，並且採用不足以識別為特定組織所使用之無線網路名稱	Basic Settings > Wireless Settings > Network Name (SSID) > Rename	Wireless Setting > Basic > SSID > Rename	Network > Wireless LAN 2.4G/5G > General > Network Name(SSID) > Rename
6	TWGCB-03-001-0006		關閉 SSID 廣播	▪ 關閉 SSID 的廣播模式，並要求使用者自行記錄連線的 SSID ▪ 這作法並不能避免有經驗的攻擊者發現 SSID，但仍應作為安全防護的一個部分	Basic Settings > Wireless Settings > SSID Visibility > Disable	Wireless Setting > Security > Broadcast SSID > Disable	Network > Wireless LAN 2.4G/5G > General > Hide SSID > Enable

顯而易見、難以達成
技服 GCB 規則

* 無線網路

10	TWGCB-03-001-0010	存取控制	啟用 MAC 位置過濾	▪如果採用自動化的裝置網路登錄，應啟用 MAC 位置過濾功能 ▪這作法並不能避免有經驗的攻擊者冒用偽裝的 MAC 進行攻擊，但仍應作為安全防護的一個部分	Filters > MAC Bypass > 設定 MAC 名單	Wireless Setting > Securiy > Additional Authentication > MAC Filter > 設定 MAC 名單	Security > Firewall > MAC Filtering Rule > Enable MAC Filtering > 設定 MAC 名單
11	TWGCB-03-001-0011		關閉 DHCP 協定	關閉 DHCP 協定，並指定固定靜態 IP 位置給每個終端使用者	DHCP Server > Static Pool Settings	Wireless Setting > Basic > IP Address Assignment > Static IP	Network > DHCP Server > General > Disable

技服 GCB 網站FAQ
作業系統 Win7

7.Adobe Acrobat Professional無法進行軟體更新，怎麼辦呢？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-001-0187設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"Windows Installer"=>"禁止非系統管理員套用廠商簽署的更新"」設為停用即可。

6.如何在Microsoft Windows 7電腦開啟遠端桌面連線共用？

Windows 10 相同狀況

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-001-0253與TWGCB-01-001-0217設定值，方法如下：

將「"電腦設定"=>"Windows設定"=>"安全性設定"=>"具有進階安全性的Windows防火牆"=>"輸入規則"」，新增防火牆輸入規則：允許「網域」TCP通訊埠3389的輸入連線，以及將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"遠端桌面服務"=>"遠端桌面工作階段主機"=>"連線"=>"允許使用者使用遠端桌面服務從遠端連線"」設為啟用即可。

技服 GCB 網站FAQ
作業系統 Win10

4.如何解決Windows市集App(如:相片、計算機)無法使用的問題？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-005-0285與TWGCB-01-005-0284設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"Windows市集"=>"安全性選項"=>"停用Windows市集中的所有應用程式"」設為啟用，以及將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"市集"=>"關閉市集應用程式"」設為停用即可。

5.如何解決Miracast投影功能無法使用的問題？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-005-0285與TWGCB-01-005-00284設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"Windows市集"=>"安全性選項"=>"停用Windows市集中的所有應用程式"」設為啟用，以及將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"市集"=>"關閉市集應用程式"」設為停用即可。

技服 GCB 網站FAQ
作業系統 Win10

13.套用政府組態基準(GCB)後，連線WiFi時顯示無網際網路，怎麼辦呢？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-005-0314、TWGCB-01-005-0325與TWGCB-01-005-0336設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"網路"=>"網路連線"=>"Windows防火牆"=>"網域設定檔"=>"Windows防火牆：禁止單點傳送回應到多點傳送或廣播要求"」設為停用，並將「"電腦設定"=>"Windows設定"=>"安全性設定"=>"具有進階安全性的Windows防火牆"=>"內容"=>"私人設定檔"=>"自訂"=>"單點傳播回應"=>"允許單點傳播回應"」設為是，以及將「"電腦設定"=>"Windows設定"=>"安全性設定"=>"具有進階安全性的Windows防火牆"=>"內容"=>"公用設定檔"=>"自訂"=>"單點傳播回應"=>"允許單點傳播回應"」設為是即可。

14.套用政府組態基準(GCB)後，購買的字型無法使用，怎麼辦呢？

1.政府組態基準(GCB)「封鎖未受信任的字型」設定，限制僅可載入安裝於「%Windir%\Fonts」資料夾之受信任字型。

2.政府組態基準(GCB)之設定值原則上不宜隨意更動，若必須調整TWGCB-01-005-0298設定值，方法如下：
將「"電腦設定"=>"系統管理範本"=>"系統"=>"緩和選項"=>"封鎖未受信任的字型"」設為停用即可。

技服 GCB 網站FAQ
瀏覽器 Chrome

11.套用Google Chrome GCB設定後，無法從Google Drive網站下載雲端硬碟檔案，該怎麼辦？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-02-003-0006設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Google Chrome"=>"封鎖第三方Cookie"」項目設為停用，即可從Google Drive網站下載檔案。

台大自行新增

* Chrome 例外管理清單

編號	原則設定名稱	GCB 建議值	變更事由
TWGCB-02-003-0027	針對遠端存取主機啟用或停用無 PIN 碼驗證機制	停用	設定後造成Google遠端桌面無法使用，故排除
TWGCB-02-003-0031	Configure the required domain names for remote access hosts		設定後造成Google遠端桌面無法使用，故排除
TWGCB-02-003-0014	啟用自動填入		影響同仁輸入表單效率，故排除。
TWGCB-02-003-0032	啟用地址的自動填入功能		影響同仁輸入表單效率，故排除。(20210906 davisyou)

台大自行新增

* Mozilla Firefox 例外管理清單

編號	原則設定名稱	GCB 建議值	變更事由
TWGCB-02-004-0032	停用JavaScript調整功能視窗(Context Windows)之功能	false	造成Google Driver 無法下載
TWGCB-02-004-0034	不接受第三方Cookie	1	造成Google Driver 無法下載
TWGCB-02-004-0037	啟用追蹤保護功能	true	造成 https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html 連結無法使用故排除

GCB 導入工具

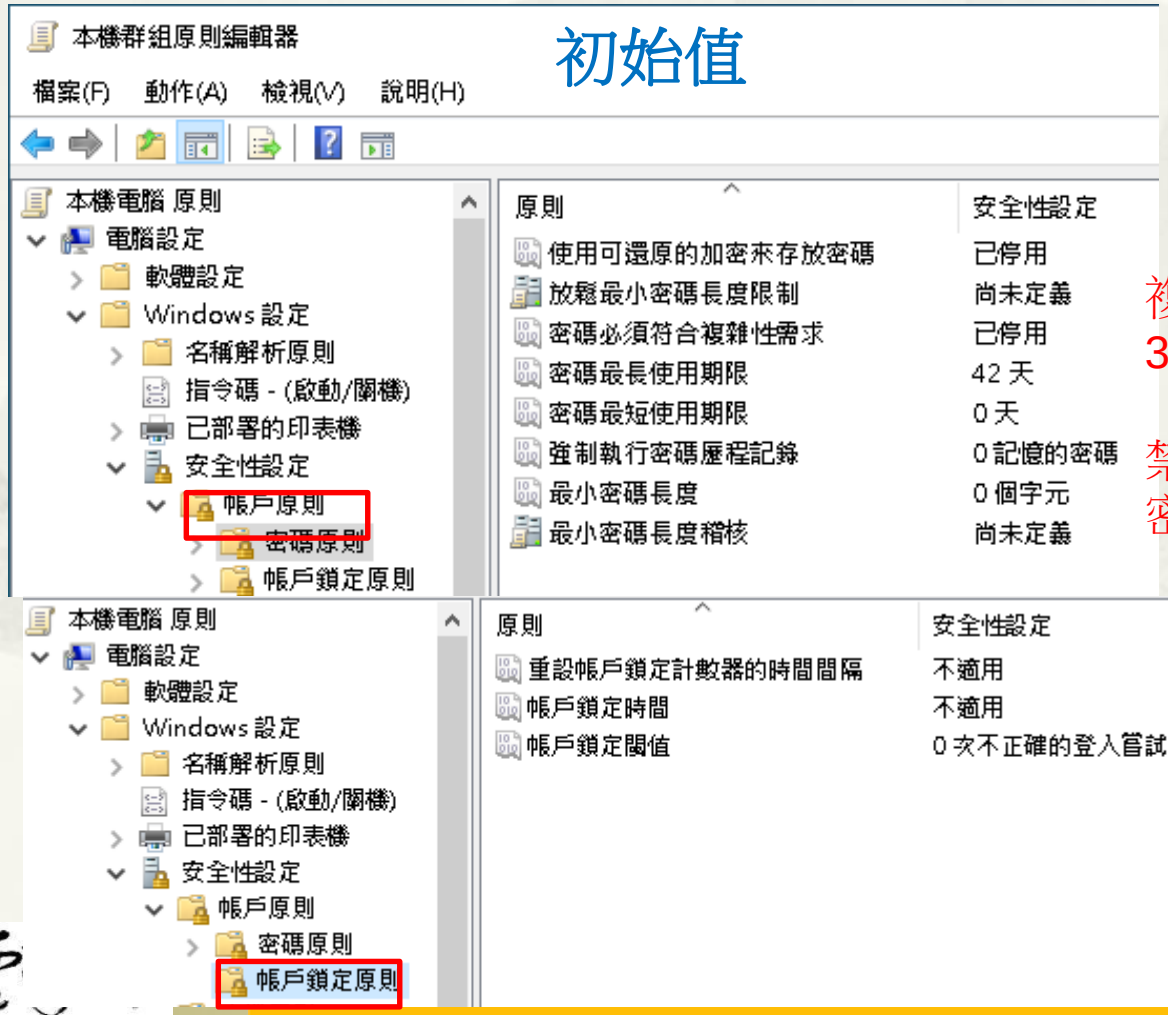
GCB 導入工具

- Local Group Policy(本機群組原則)編輯器 gpedit.msc
  - 手動逐項設定
- 微軟群組原則批次匯入程式 LGPO.exe
  - LGPO.exe 備份匯出 GPO 檔案
  - LGPO.exe 匯入 GPO 檔案
  - LGPO.exe 匯入 PolicyRules

本機群組原則編輯器
gpedit.msc

帳戶原則

* gpedit.msc



初始值

複雜密碼設置原則
3個月內變更一次密碼

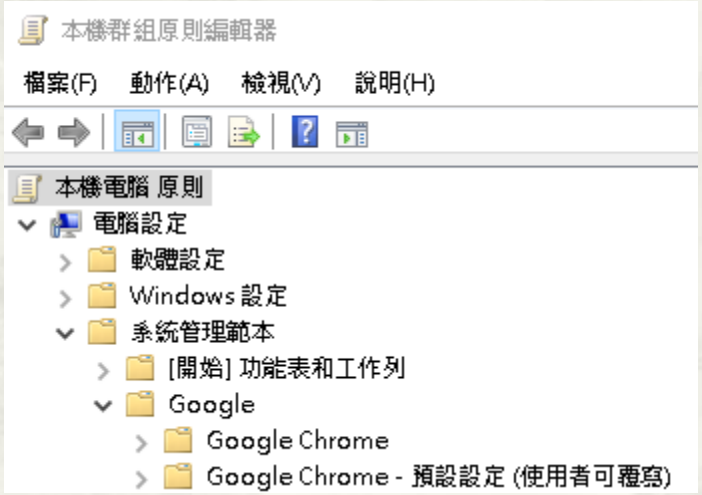
禁止重複使用相同的密碼
密碼的長度最少應有8位長度

Chrome 系統管理範本匯入

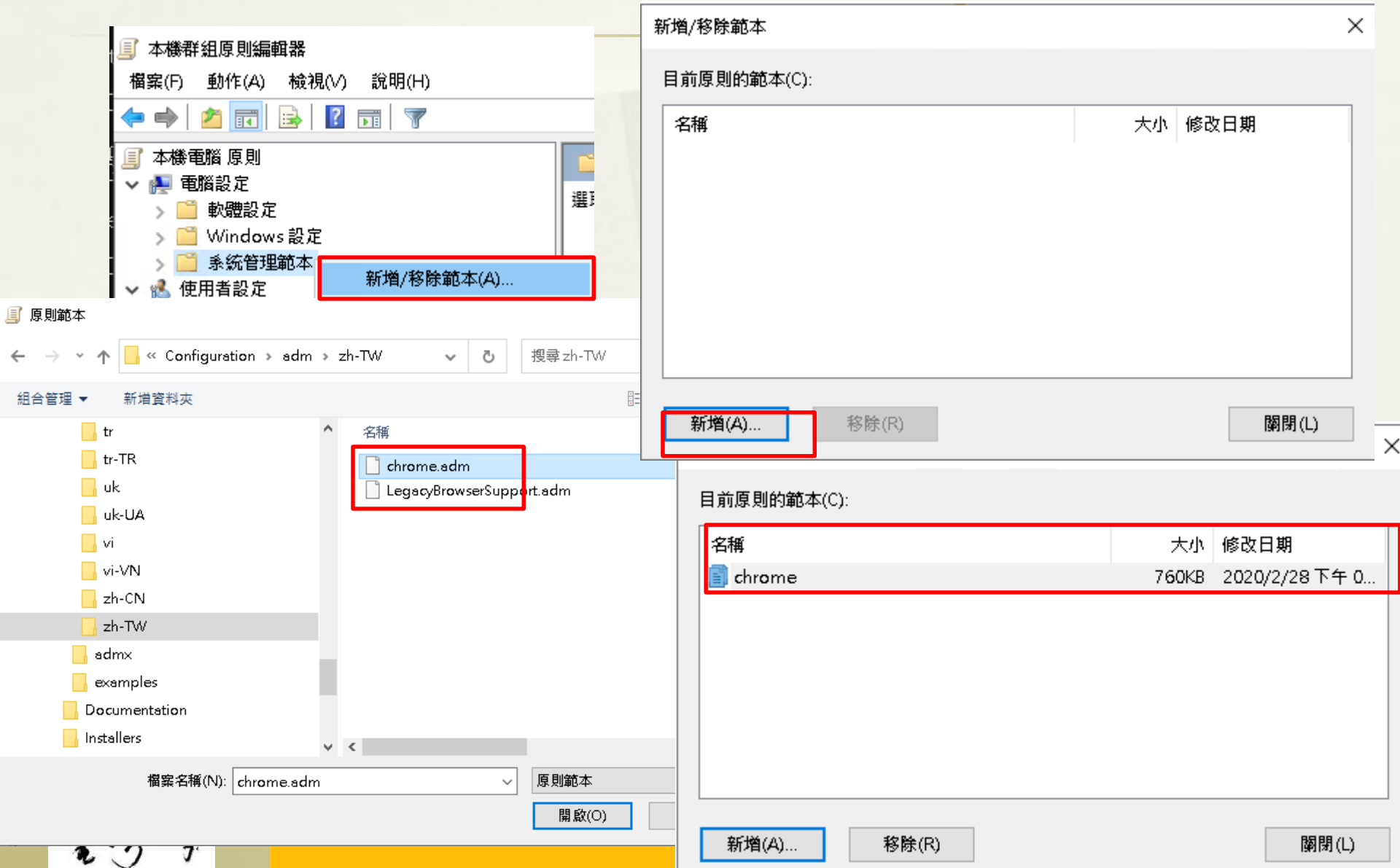
- 下載 Chrome 政策範本 .ADM .ADMX
  - 為受管理的電腦設定 Chrome 瀏覽器政策
    - https://support.google.com/chrome/a/answer/187202?hl=zh-Hant#zippy=%2Cwindows
  - Google Chrome 範本和說明文件的 ZIP 檔案
    - https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip

安裝方法1

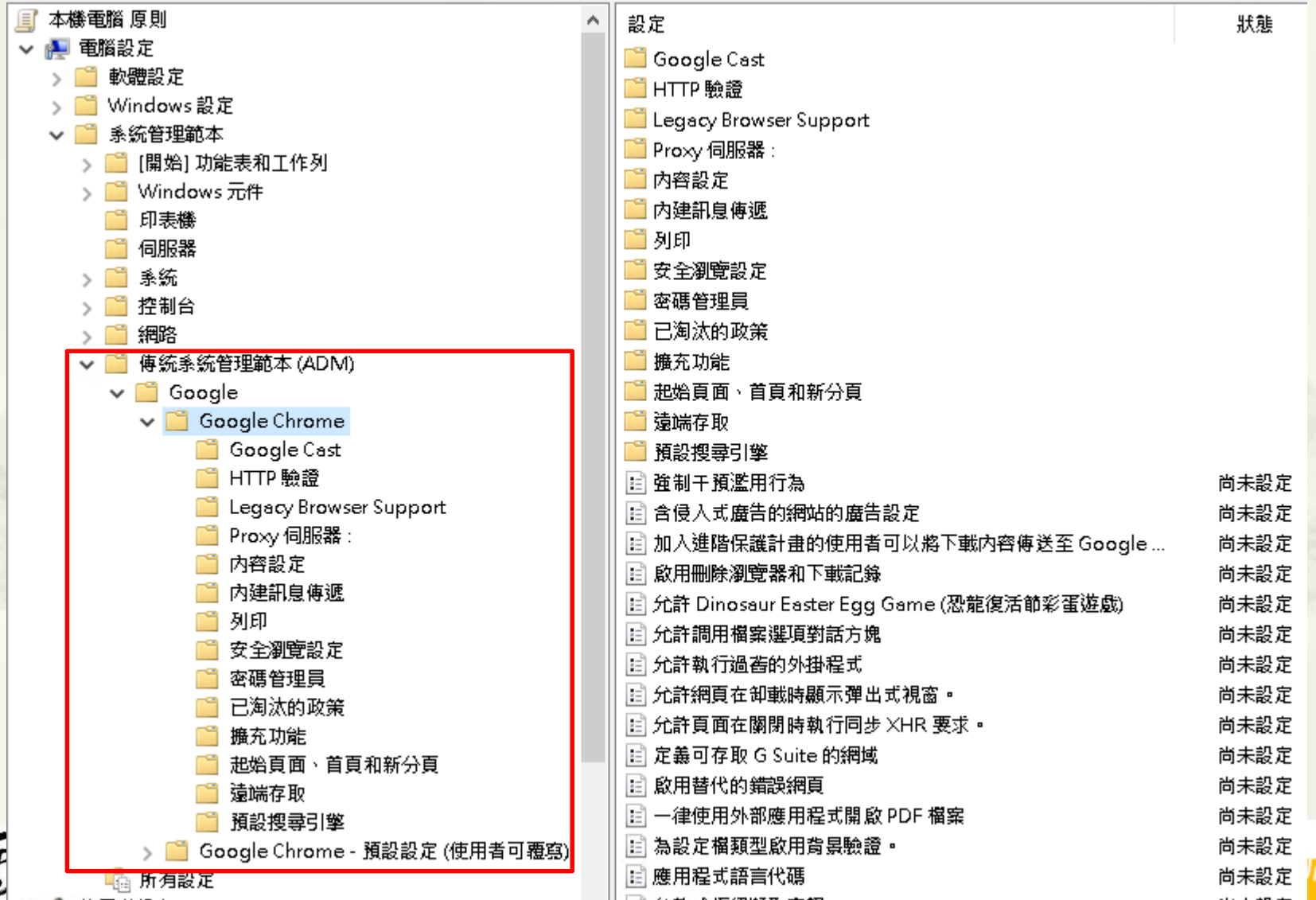
* Copy .\windows\admx\chrome.admx To C:\Windows\PolicyDefinitions
* Copy .\windows\admx\zh-TW\chrome.adml To C:\Windows\PolicyDefinitions\zh-TW



安裝方法2


本機群組原則編輯器
檔案(F) 動作(A) 檢視(V) 說明(H)
本機電腦 原則
電腦設定
軟體設定
Windows 設定
系統管理範本
使用者設定
新增/移除範本(A)...
新增/移除範本
目前原則的範本(C):
名稱
大小
修改日期
新增(A)...
移除(R)
關閉(L)
原則範本
« Configuration › adm › zh-TW
搜尋 zh-TW
組合管理
新增資料夾
tr
tr-TR
uk
uk-UA
vi
vi-VN
zh-CN
zh-TW
admx
examples
Documentation
Installers
名稱
chrome.adm
LegacyBrowserSupport.adm
檔案名稱(N): chrome.adm
原則範本
開啟(O)
目前原則的範本(C):
名稱
大小
修改日期
chrome
760KB
2020/2/28 下午 0...
新增(A)...
移除(R)
關閉(L)

安裝方法2


本機電腦 原則
電腦設定
軟體設定
Windows 設定
系統管理範本
[開始] 功能表和工作列
Windows 元件
印表機
伺服器
系統
控制台
網路
傳統系統管理範本 (ADM)
Google
Google Chrome
Google Cast
HTTP 驗證
Legacy Browser Support
Proxy 伺服器
內容設定
內建訊息傳遞
列印
安全瀏覽設定
密碼管理員
已淘汰的政策
擴充功能
起始頁面、首頁和新分頁
遠端存取
預設搜尋引擎
Google Chrome - 預設設定 (使用者可覆寫)
所有設定
設定
狀態
Google Cast
HTTP 驗證
Legacy Browser Support
Proxy 伺服器
內容設定
內建訊息傳遞
列印
安全瀏覽設定
密碼管理員
已淘汰的政策
擴充功能
起始頁面、首頁和新分頁
遠端存取
預設搜尋引擎
強制干預濫用行為 尚未設定
含侵入式廣告的網站的廣告設定 尚未設定
加入進階保護計畫的使用者可以將下載內容傳送至 Google ... 尚未設定
啟用刪除瀏覽器和下載記錄 尚未設定
允許 Dinosaur Easter Egg Game (恐龍復活節彩蛋遊戲) 尚未設定
允許調用檔案選項對話方塊 尚未設定
允許執行過舊的外掛程式 尚未設定
允許網頁在卸載時顯示彈出式視窗。 尚未設定
允許頁面在關閉時執行同步 XHR 要求。 尚未設定
定義可存取 G Suite 的網域 尚未設定
啟用替代的錯誤網頁 尚未設定
一律使用外部應用程式開啟 PDF 檔案 尚未設定
為設定檔類型啟用背景驗證。 尚未設定
應用程式語言代碼 尚未設定

Firefox

表2　Mozilla Firefox 政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方式	GCB 設定值	備註
1	TWGCB-02-004-0001	Updating Firefox	啟用更新功能	當有更新版本釋出時，此項設定可決定Firefox是否進行自動更新作業	於 CFG 檔案中，新增設定：lockPref("app.update.enabled", true);	true	
2	TWGCB-02-004-0002	Updating Firefox	啟用自動下載更新與安裝	當有更新版本釋出時，此項設定可決定是否進行自動下載與執行安裝更新版本作業	於 CFG 檔案中，新增設定：lockPref("app.update.auto", true);	true	
3	TWGCB-02-004-0003	Updating Firefox	啟用更新下載暫存整備區(Staging Area)	當有更新版本釋出且進行下載時，此項設定可決定Firefox 於更新檔案下載時，將更新暫存檔於暫存整備區(Staging Area)中，待更新檔案下載完成後即可進行安裝作業	於 CFG 檔案中，新增設定：lockPref("app.update.staging.enabled", true);	true	

Firefox

- ds_mozilla.cfg 放置位置
  - C:\Program Files\Mozilla Firefox (64位元)
  - C:\Program Files (x86)\Mozilla Firefox (32位元)
- local-settings.js 放置位置
  - C:\Program Files\Mozilla Firefox\defaults\pref (64位元)
  - C:\Program Files (x86) \Mozilla Firefox\defaults\pref (32位元)

微軟群組原則批次匯入程式 LGPO.exe

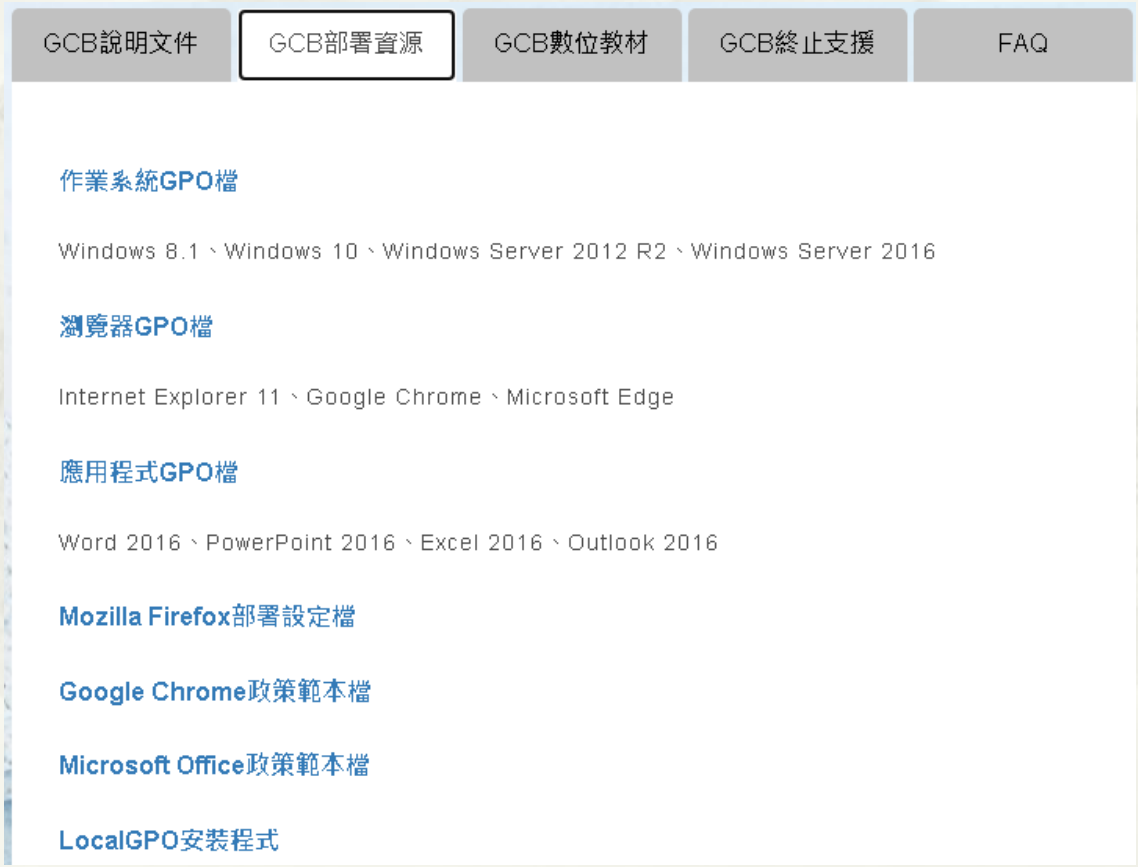
LGPO.exe 備份匯出 GPO 檔案

LGPO.exe 匯入 GPO 檔案

LGPO.exe 匯入 PolicyRules

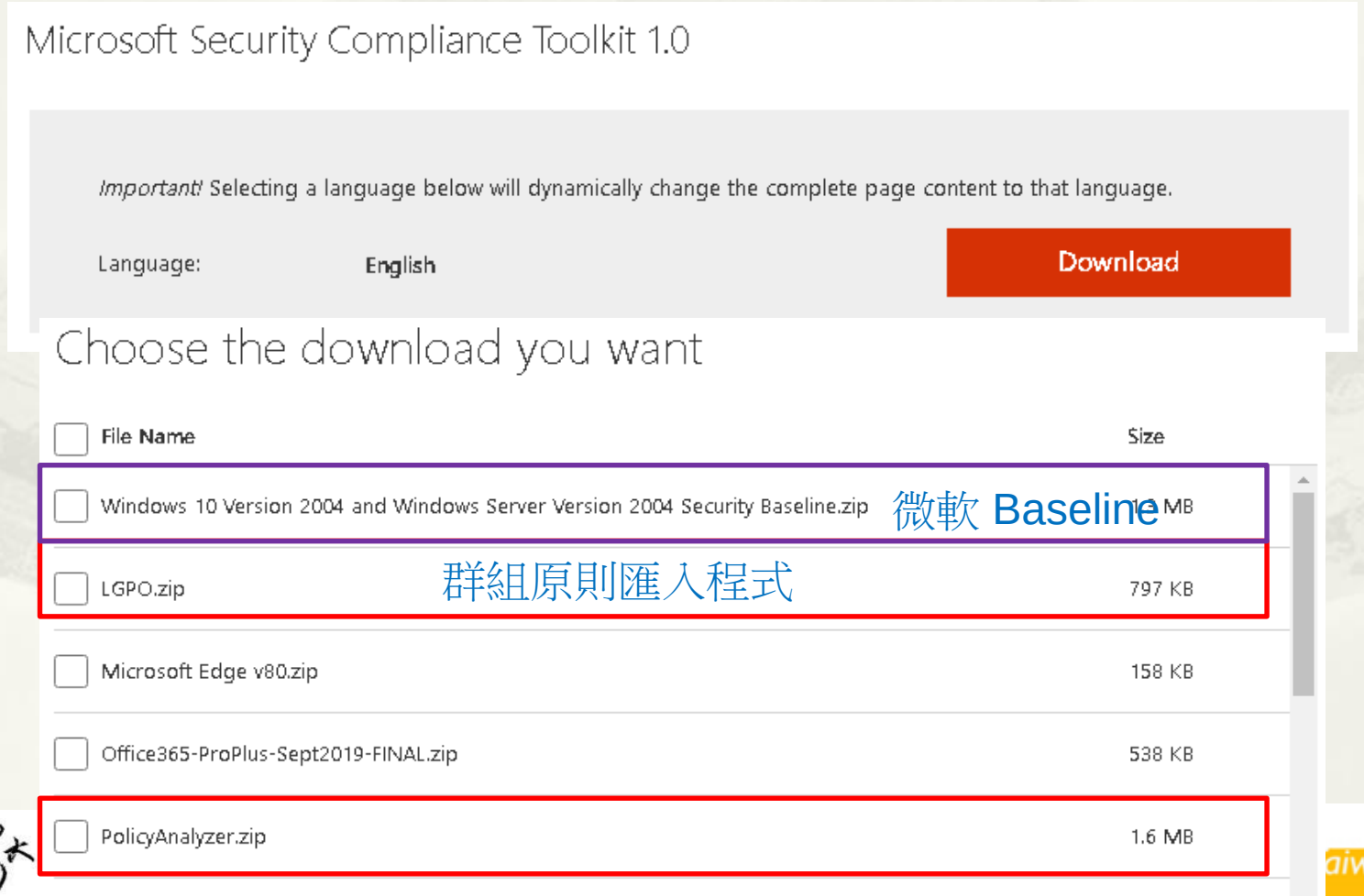
技服 GPO 設定檔下載

* https://www.nccst.nat.gov.tw/GCB?lang=zh



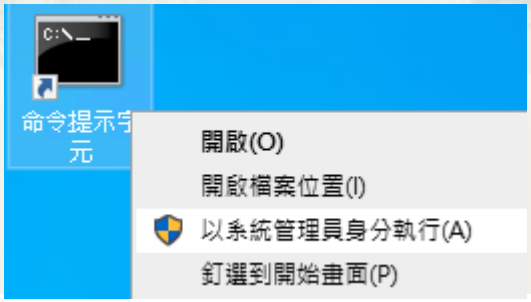
微軟 Security Compliance Toolkit

* Microsoft Security Compliance Toolkit 1.0
* https://www.microsoft.com/en-us/download/details.aspx?id=55319



群組原則匯入程式
LGPO v3.0

- a command-line utility that is designed to help automate management of Local Group Policy.
- Support import from
  - Registry Policy (Registry.pol) files
  - Security Templates (.ini)
  - Advanced Auditing backup files
  - LGPO text
  - .PolicyRules Policy Analyzer
  - XML files
- 開啟命令提示字元(系統管理者身份)



LGPO.exe 備份匯出 GPO 檔案

* 備份目前組態
  * LGPO.exe /b C:\GCB\backup

LGPO.exe 匯入 GPO 檔案

- 全部導入
  - LGPO.exe /g .\GCB-Windows10-gpos
- 部分導入， Only AccountSettings
  - LGPO.exe /g .\GCB-Windows10-gpos\Windows10AccountSettings

```
C:\LGPO>LGPO /g C:\GCB-Windows10-gpos
LGPO.exe v2.2 - Local Group Policy Object utility

Apply security template: C:\GCB-Windows10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}\DomainSysvol\GPO\Ma
chine\microsoft\windows nt\SecEdit\GptTmpl.inf
Created directory for audit policy
Copied C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1BC7}\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:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1B
C7}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1
BC7}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Apply security template: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{E12EA9E0-D8AB-4EB8-818A
-E521D26A470F}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{E12EA
9E0-D8AB-4EB8-818A-E521D26A470F}\DomainSysvol\GPO\Machine\registry.pol
Apply security template: C:\GCB-Windows10-gpos\Windows10FirewallSettings\{370D17DB-6E02-46A0-816F-9BF347BB6713}\DomainSysvol\GPO\M
achine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GCB-Windows10-gpos\Windows10FirewallSettings\{370D17DB-6E02-46A0-816F-9BF347BB6713}\
DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\GCB-Windows10-gpos\Windows10UserSettings\{591F3C24-5250-4F47-A19F-55B3C78E147D}\DomainS
ysvol\GPO\User\registry.pol
```

匯入後更新

- By default, Microsoft Windows refreshes its policy settings every 90 minutes with a random 30 minutes offset
- Manual Refresh the group policy
  - gpupdate /force
- C:\>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。

- 作用 : Sync *.pol to registry
  - C:\Windows\System32\GroupPolicy\Machine\Registry.pol
  - C:\Windows\System32\GroupPolicy\User\Registry.pol
  - HKEY_CURRENT_USER\Software\Policies
  - HKEY_LOCAL_MACHINE\Software\Policies

LGPO.exe 匯入 PolicyRules

- Import from a Policy Analyzer .PolicyRules file:
  - LGPO.exe /p C:\GCB\GCB.PolicyRules

微軟 PolicyAnalyzer

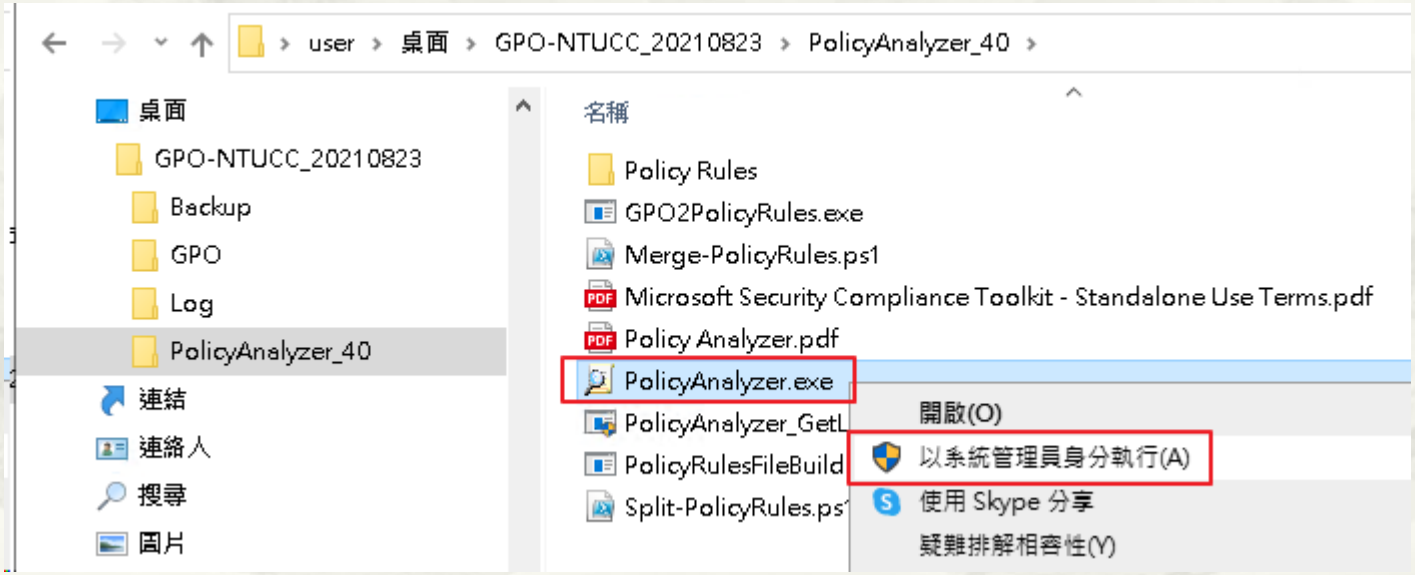
※不支援登入帳號有中文字元

※不支援檔案及路徑有中文字元

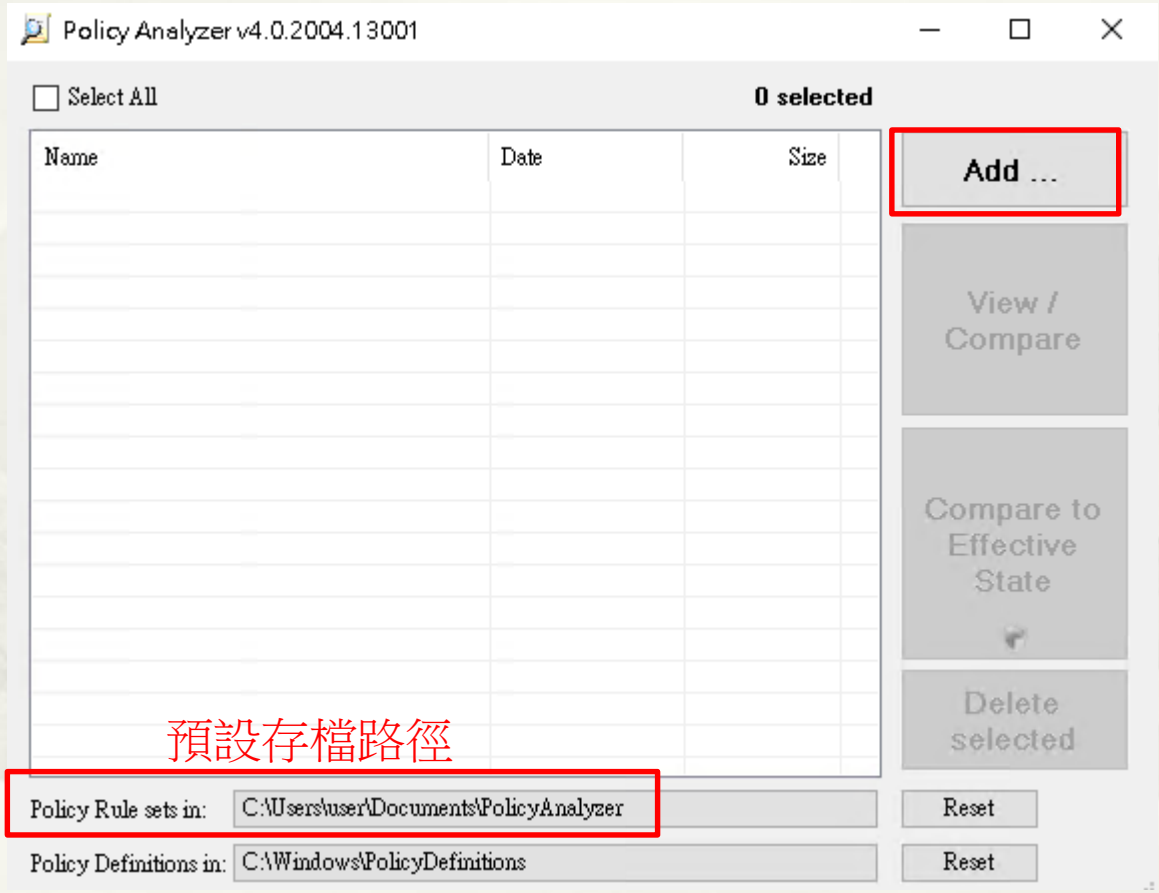
GPO 檔案匯入

執行 PolicyAnalyzer.exe

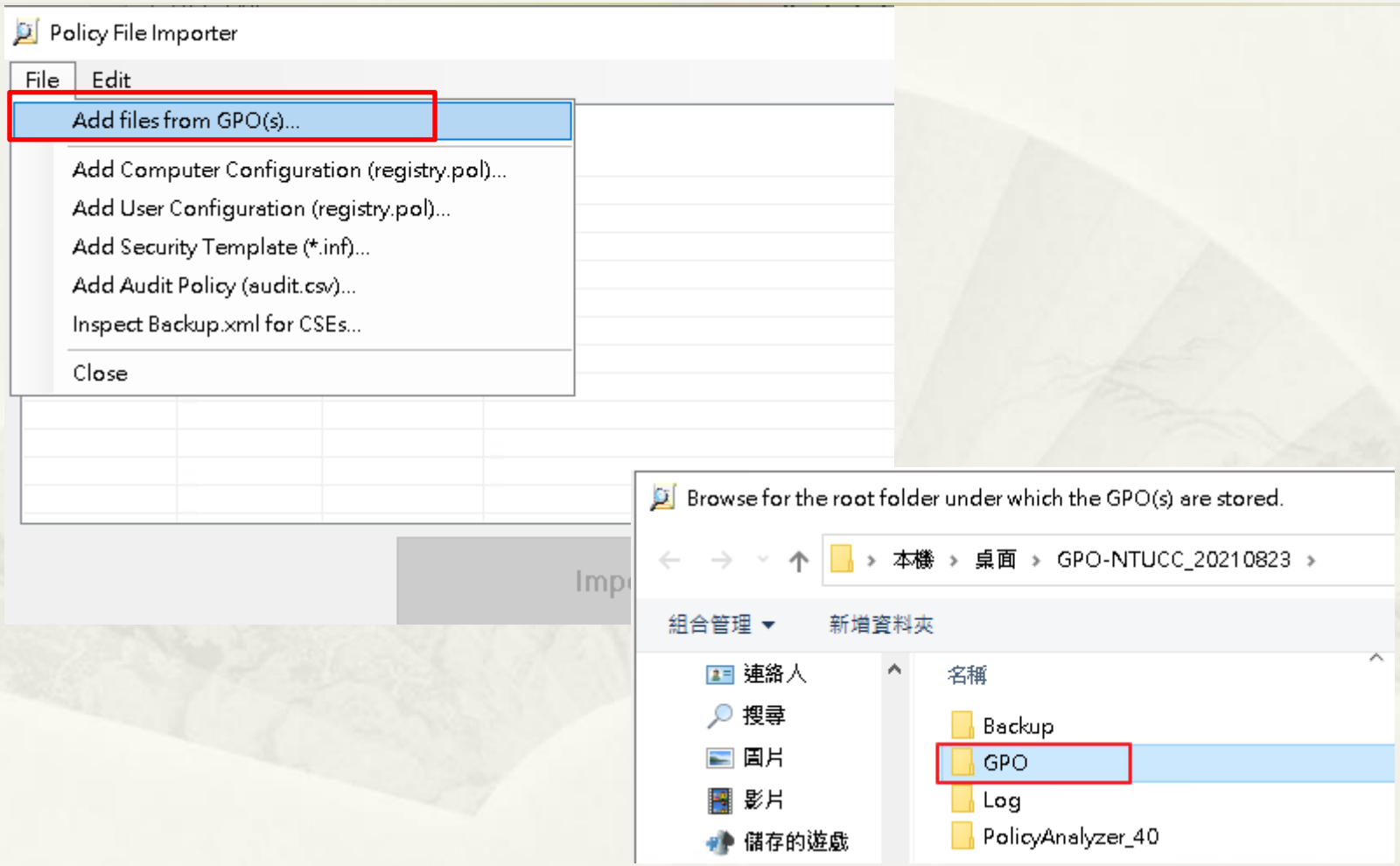
* 系統管理者權限執行 \PolicyAnalyzer_40\PolicyAnalyzer.exe



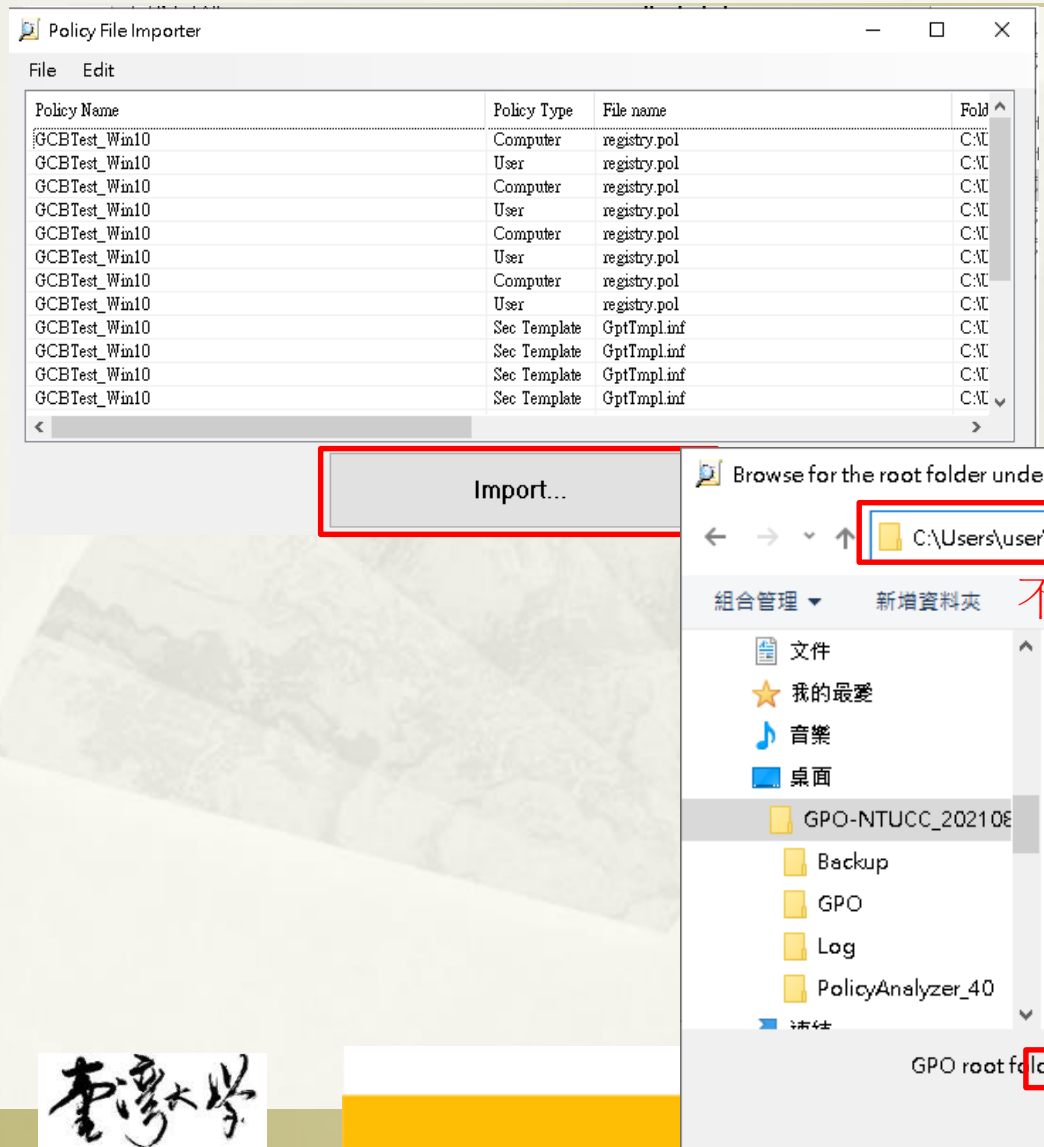
PolicyAnalyzer
Add GPO files



PolicyAnalyzer
Add GPO files



PolicyAnalyzer
產生 .PolicyRules 檔案

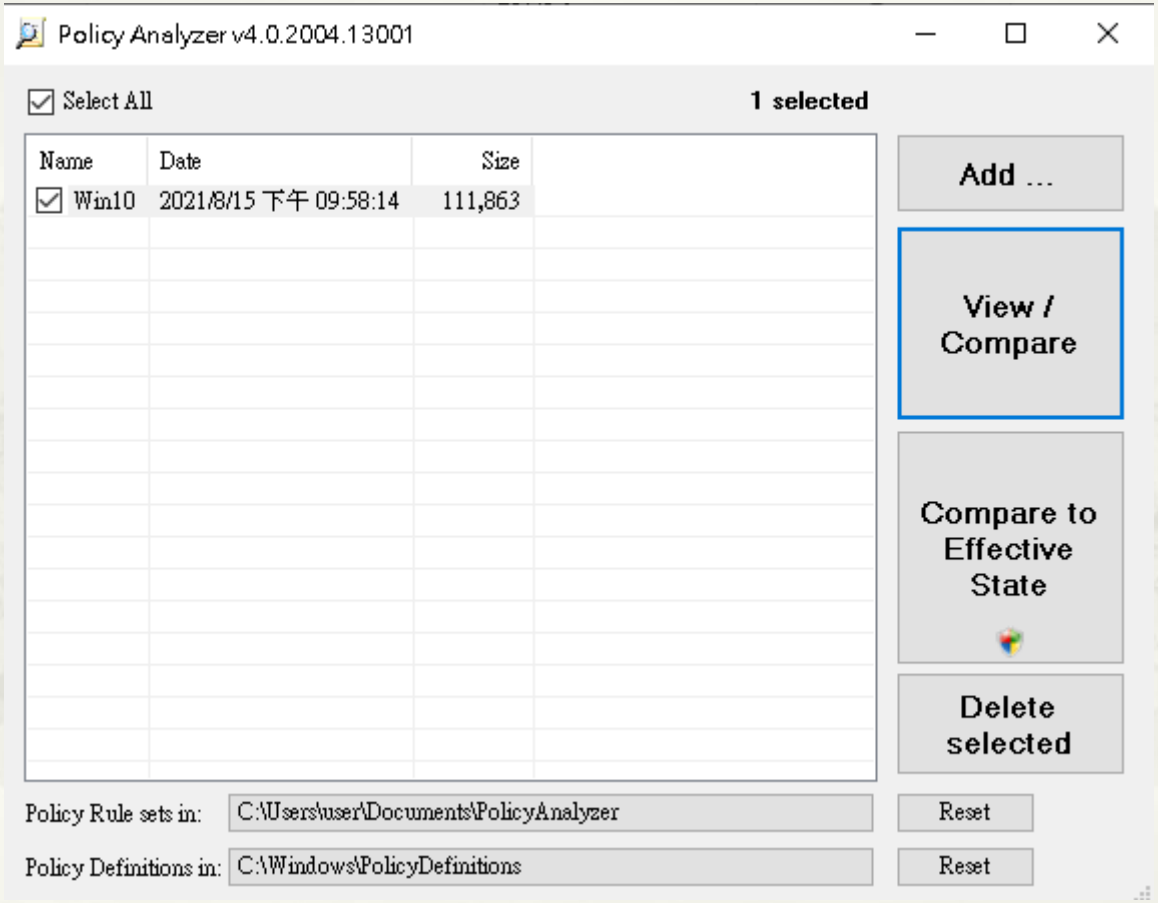


.PolicyRules 檔案內容

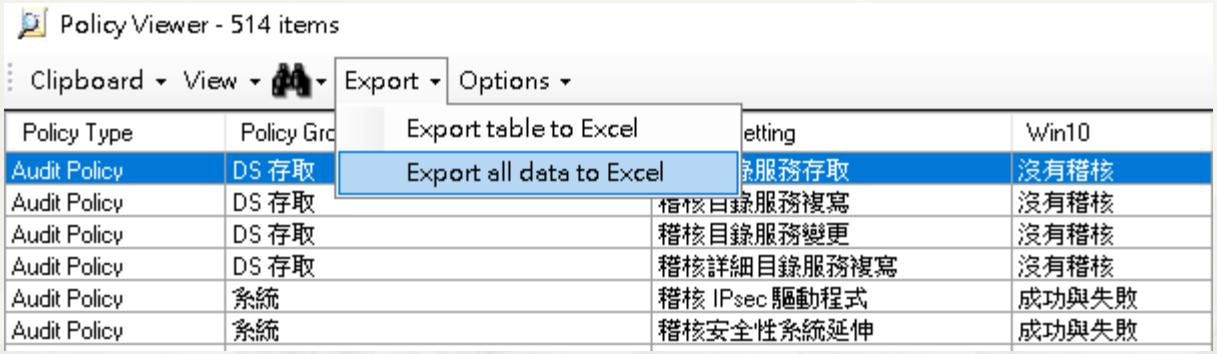
- C:\Users\user\Documents\PolicyAnalyzer\GPO.PolicyRules

<ComputerConfig><Key>Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging</Key><Value>LogFilePath</Value><RegType>REG_SZ
<ComputerConfig><Key>Software\Policies\Microsoft\WindowsMediaPlayer</Key><Value>GroupPrivacyAcceptance</Value><RegType>REG_DWORD</Re
<ComputerConfig><Key>Software\Policies\Microsoft\WindowsMediaPlayer</Key><Value>DisableAutoUpdate</Value><RegType>REG_DWORD</RegType>
<ComputerConfig><Key>Software\Policies\Microsoft\WMDRM</Key><Value>DisableOnline</Value><RegType>REG_DWORD</RegType><RegData>1</RegD
<ComputerConfig><Key>System\CurrentControlSet\Policies\EarlyLaunch</Key><Value>DriverLoadPolicy</Value><RegType>REG_DWORD</RegType><
<UserConfig><Key>Software\Microsoft\Windows\CurrentVersion\Policies\Attachments</Key><Value>SaveZoneInformation</Value><RegType>REG_
<UserConfig><Key>Software\Microsoft\Windows\CurrentVersion\Policies\Attachments</Key><Value>HideZoneInfoOnProperties</Value><RegType>
<UserConfig><Key>Software\Microsoft\Windows\CurrentVersion\Policies\Attachments</Key><Value>ScanWithAntiVirus</Value><RegType>REG_DWO
<UserConfig><Key>Software\Microsoft\Windows\CurrentVersion\Policies\System</Key><Value>NoDispScrSavPage</Value><RegType>REG_DWORD</R
<UserConfig><Key>Software\Policies\Microsoft\Assistance\Client\1.0</Key><Value>NoExplicitFeedback</Value><RegType>REG_DWORD</RegType>
<UserConfig><Key>Software\Policies\Microsoft\Internet Connection Wizard</Key><Value>DisableICW</Value><RegType>REG_DWORD</RegType><R
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Control Panel</Key><Value>FormSuggest</Value><RegType>REG_DWORD</RegT
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Control Panel</Key><Value>FormSuggest Passwords</Value><RegType>REG_D
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Main</Key><Value>Use FormSuggest</Value><RegType>REG_SZ</RegType><Regl
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Main</Key><Value>FormSuggest Passwords</Value><RegType>REG_SZ</RegTyp
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Main</Key><Value>FormSuggest PW Ask</Value><RegType>REG_SZ</RegType><
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Main</Key><Value>Page_Transitions</Value><RegType>REG_DWORD</RegType>
<UserConfig><Key>Software\Policies\Microsoft\Internet Explorer\Restrictions</Key><Value>NoExternalBranding</Value><RegType>REG_DWORD
<UserConfig><Key>Software\Policies\Microsoft\Windows\Control Panel\Desktop</Key><Value>ScreenSaveActive</Value><RegType>REG_SZ</RegT
<UserConfig><Key>Software\Policies\Microsoft\Windows\Control Panel\Desktop</Key><Value>ScreenSaverIsSecure</Value><RegType>REG_SZ</R
<UserConfig><Key>Software\Policies\Microsoft\Windows\Control Panel\Desktop</Key><Value>ScreenSaveTimeOut</Value><RegType>REG_SZ</Reg
<UserConfig><Key>Software\Policies\Microsoft\Windows\Control Panel\Desktop</Key><Value>SCRNSAVE.EXE</Value><RegType>REG_SZ</RegType>
<UserConfig><Key>Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications</Key><Value>NoToastApplicationNotificationOnLo
<UserConfig><Key>Software\Policies\Microsoft\WindowsMediaPlayer</Key><Value>PreventCodecDownload</Value><RegType>REG_DWORD</RegType>
<SecurityTemplate Section="System Access"><LineItem>MinimumPasswordAge=1</LineItem><SourceFile>C:\Users\user\Desktop\GCB_Creator\GPO
<SecurityTemplate Section="System Access"><LineItem>MaximumPasswordAge=90</LineItem><SourceFile>C:\Users\user\Desktop\GCB_Creator\GP
<SecurityTemplate Section="System Access"><LineItem>MinimumPasswordLength=8</LineItem><SourceFile>C:\Users\user\Desktop\GCB_Creator\
<SecurityTemplate Section="System Access"><LineItem>PasswordComplexity=1</LineItem><SourceFile>C:\Users\user\Desktop\GCB_Creator\GPO
<SecurityTemplate Section="System Access"><LineItem>PasswordHistorySize=3</LineItem><SourceFile>C:\Users\user\Desktop\GCB_Creator\GP

PolicyAnalyzer View/Compare



PolicyAnalyzer
Export all data to Excel



* Excel

Policy Config	Policy Path	Policy Setting Name	Policy Type	Policy Group or Registry Key	Policy Setting	GPO	GPO Optio	GPO Type	Explain Text	GPO GPO
安全性設定	本機原則\安全性選項	Microsoft 網路用戶端: 數位簽	HKLM	System\CurrentControlSet\Services\LanmanWorkstati	EnableSecuritySignature	1	已啟用	REG_DWORD	Microsoft 網路用戶端: 為通訊加上數位簽章 (若伺服器同意) 此安全性設定決定 SMB 用戶端是否嘗試交涉 SMB 封包簽署。 伺服器訊息區 (SMB) 通訊協定是 Microsoft 檔案及列印共用與許多其他網路作業 (例如遠端 Windows 系統管理) 的基礎。為防止會修改傳輸中 SMB 封包的攔截式攻擊，SMB 通訊協定支援 SMB 封包的數位簽署。此原則設定決定 SMB 用戶端元件連線至 SMB 伺服器時，是否嘗試交涉 SMB 封包簽署。 若啟用此設定，Microsoft 網路用戶端將於建立工作階段時要求伺服器執行 SMB 封包簽署。若已在伺服器上啟用封包簽署，將會交涉封包簽署。若停用此原則，SMB 用戶端將不會交涉 SMB 封包簽署。 預設值: 已啟用。 注意 所有 Windows 作業系統都支援用戶端 SMB 元件與伺服器端 SMB 元件。在 Windows 2000 與更新版本的作業系統上，啟用或要求用戶端與伺服器端 SMB 元件的封包簽署是由下列四個原則設定所控制: Microsoft 網路用戶端: 為通訊加上數位簽章 (一律) - 控制用戶端	GCBTest_Win10

與 GPO.PolicyRules 比對進行修改

GCB 導入方法

GCB 導入方法

- 方法1
  - 準備一台新安裝 Windows 10 電腦
  - 依據技服網站"GCB文件"逐項設定(已考慮排除項)
    - Gpedit.msc
  - 使用 LGPO 進行 GPO 備份
    - LGPO.exe /b C:\GCB\GPO
  - 於其他電腦使用 LGPO 匯入GPO
    - LGPO.exe /g C:\GCB\GPO
    - gpupdate /force

GCB 導入方法

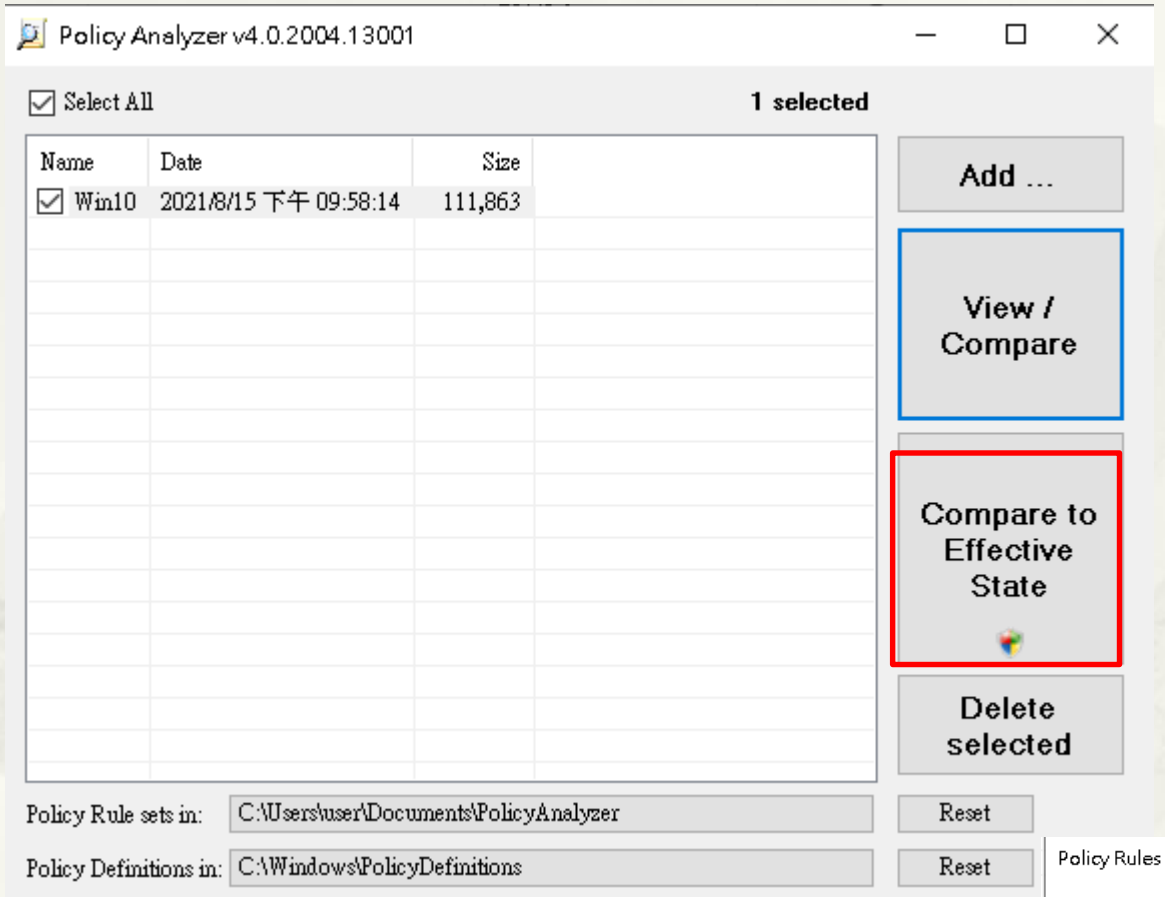
- 方法2
  - 準備一台新安裝 Windows 10 電腦
  - 技服網站 “GCB部署資源”下載 GPO檔案
  - 執行 LGPO.exe 匯入 GPO
    - LGPO /g C:\GCB\GPO
    - gpupdate /force
  - 依據排除項逐項進行調整
    - Gpedit.msc
  - 使用 LGPO 進行 GPO 備份
    - LGPO.exe /b C:\GCB\GPO
  - 於其他電腦使用 LGPO 匯入GPO
    - LGPO.exe /g C:\GCB\GPO
    - gpupdate /force

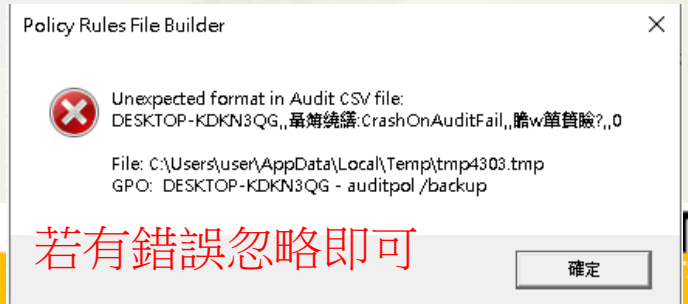
GCB 導入方法

* 方法3
  * 技服網站 “GCB部署資源”下載 GPO檔案
  * 執行 PolicyAnalyzer.exe Add GPO 檔案，存成 .PolicyRules 及 Export to Excel(文件檔)
  * 依據排除項逐項同步調整 .PolicyRules 及 Excel
  * 於其他電腦使用 LGPO 匯入PolicyRules
    * LGPO /p C:\GCB\GCB.PolicyRules
    * gpupdate /force

GCB 套用後檢測方法
微軟 PolicyAnalyzer

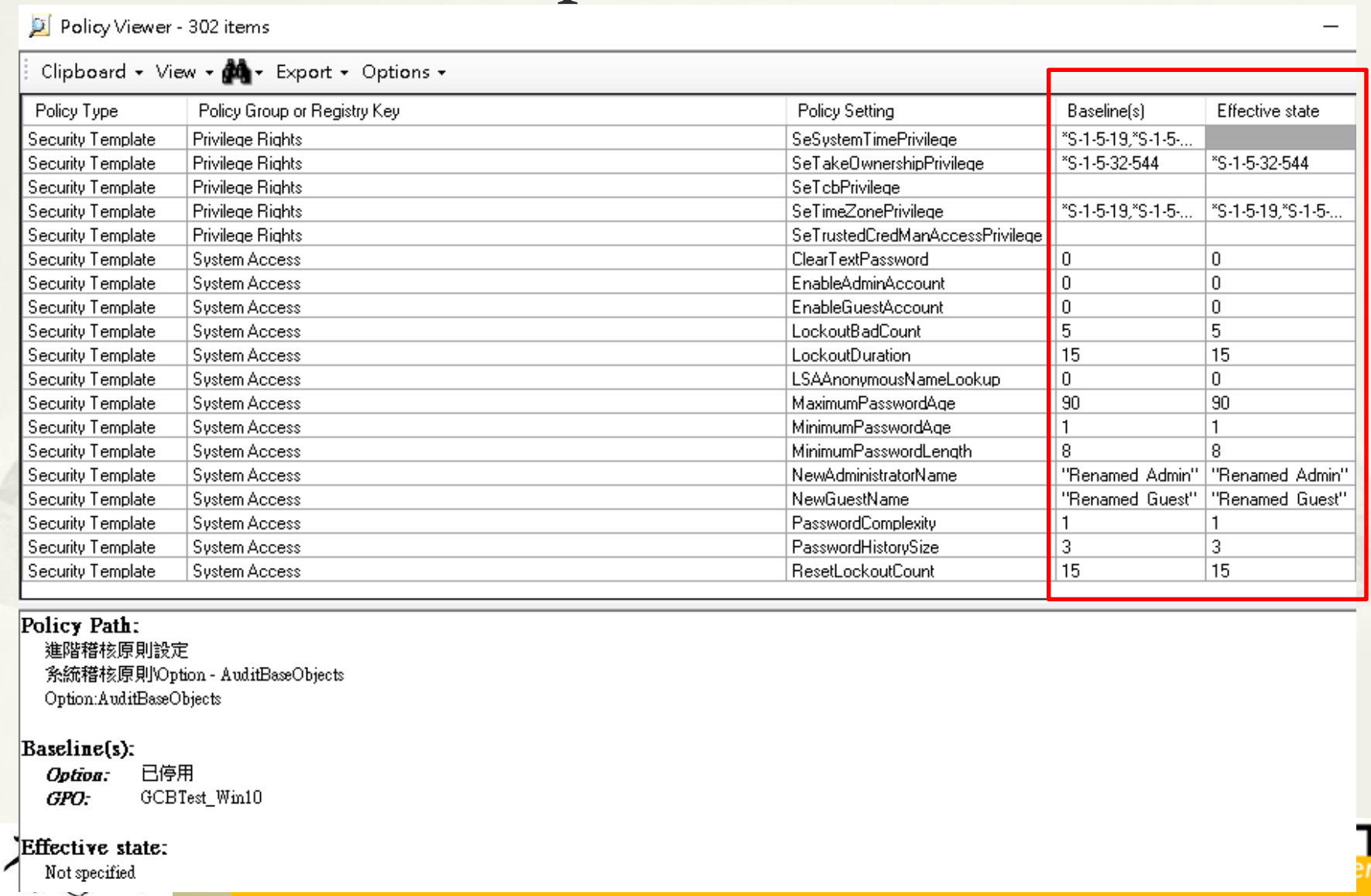
PolicyAnalyzer
Compare to 當前電腦設定



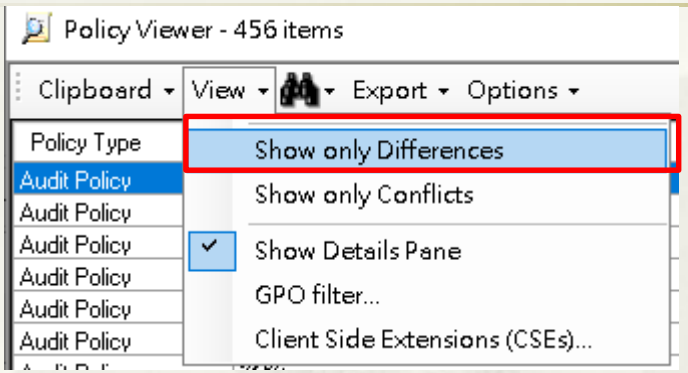


若有錯誤忽略即可

PolicyAnalyzer Compare Results



PolicyAnalyzer
Show only Differences



* 請將此畫面截圖後寄給各組檢核窗口

Policy Viewer - 5 items

Clipboard ▾ View ▾ Export ▾ Options ▾

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Option - AuditBaseObjects	Option:AuditBaseObjects	已停用	
Audit Policy	Option - CrashOnAuditFail	Option:CrashOnAuditFail	已停用	
Audit Policy	Option - FullPrivilegeAuditing	Option:FullPrivilegeAuditing	已停用	
HKLM	System\CurrentControlSet\Control\Lsa	FullPrivilegeAuditing	0	00
Security Template	Privilege Rights	SeSystemTimePrivilege	*S-1-5-19,*S-1-5-...	

技服GCB vs. 微軟Baseline

Policy Type	Policy Group or Registry Key	Policy Setting	GCB-Windows10-gpos	Windows-10-Windows Server-v2004-Security-Baseline-FINAL
Audit Policy	DS 存取	稽核目錄服務存取		失敗
Audit Policy	DS 存取	稽核目錄服務變更		成功
Audit Policy	系統	稽核 IPsec 驅動程式	成功與失敗	
Audit Policy	系統	稽核安全性系統延伸	成功與失敗	成功
Audit Policy	系統	稽核安全性狀態變更	成功與失敗	成功
Audit Policy	系統	稽核系統完整性	成功與失敗	成功與失敗
Audit Policy	系統	稽核其他系統事件	失敗	成功與失敗
Audit Policy	物件存取	稽核其他物件存取事件		成功與失敗
Audit Policy	物件存取	稽核抽取式存放裝置	成功	成功與失敗
Audit Policy	物件存取	稽核詳細的檔案共用		失敗
Audit Policy	物件存取	稽核檔案共用		成功與失敗
Audit Policy	原則變更	稽核 MPSSVC 規則層級原則變更		成功與失敗
Audit Policy	原則變更	稽核「稽核原則變更」	成功與失敗	成功
Audit Policy	原則變更	稽核其他原則變更事件		失敗
Audit Policy	原則變更	稽核驗證原則變更	成功	成功
Audit Policy	特殊權限使用	稽核機密特殊權限使用	成功與失敗	成功與失敗
Audit Policy	帳戶登入	稽核 Kerberos 服務票證操作		失敗
Audit Policy	帳戶登入	稽核 Kerberos 驗證服務		成功與失敗
Audit Policy	帳戶登入	稽核認證驗證	成功與失敗	***CONFLICT***
Audit Policy	帳戶管理	稽核安全性群組管理	成功與失敗	成功
Audit Policy	帳戶管理	稽核使用者帳戶管理	成功與失敗	成功與失敗
Audit Policy	帳戶管理	稽核其他帳戶管理事件	成功與失敗	成功
Audit Policy	帳戶管理	稽核電腦帳戶管理	成功	成功
Audit Policy	登入/登出	稽核其他登入/登出事件		成功與失敗
Audit Policy	登入/登出	稽核特殊登入	成功	成功
Audit Policy	登入/登出	稽核帳戶鎖定	成功與失敗	失敗
Audit Policy	登入/登出	稽核登入	成功與失敗	成功與失敗
Audit Policy	登入/登出	稽核登出	成功	
Audit Policy	登入/登出	稽核群組成員資格		成功
Audit Policy	詳細追蹤	稽核 PNP 活動		成功
Audit Policy	詳細追蹤	稽核建立處理程序	成功	成功

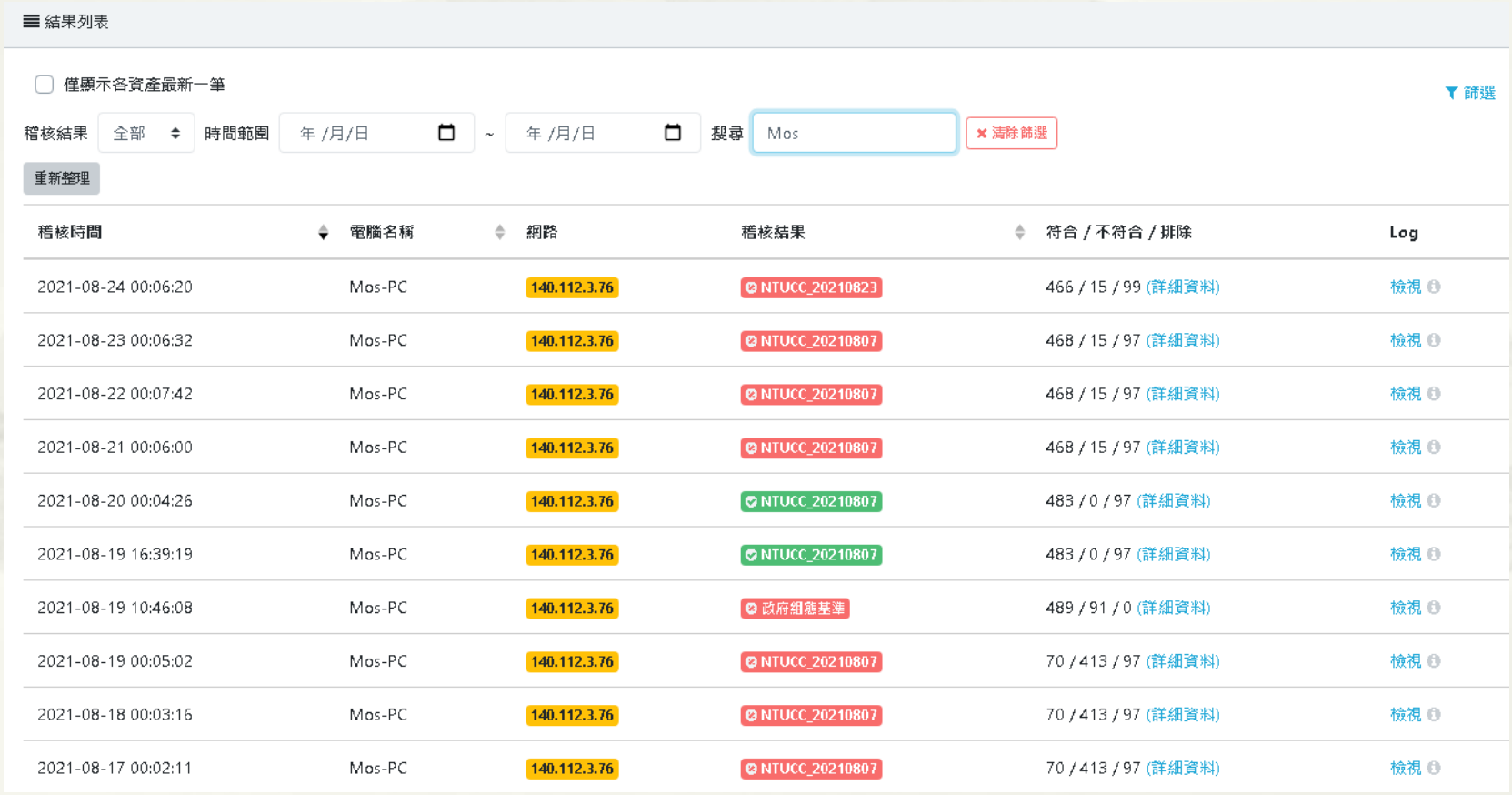
GCB 套用前後差異

注意事項

* 一台電腦多個帳號
  * 僅需一個帳戶導入 GCB，其他帳戶皆合規
* 原先合規，但過幾天後變成不合規
  * 手動更改設定
  * Windows10 大版本更新(1909 -> 20H2)
  * 原先沒有安裝 Chrome, Firefox，導入 GCB 後才安裝。

Windows 10 大版本更新
19H1 -> 20H2

* 會造成部分已套用規則變成不合規



結果列表

僅顯示各資產最新一筆

篩選

稽核結果 全部 時間範圍 年 /月/日 ~ 年 /月/日 搜尋 Mos 清除篩選

重新整理

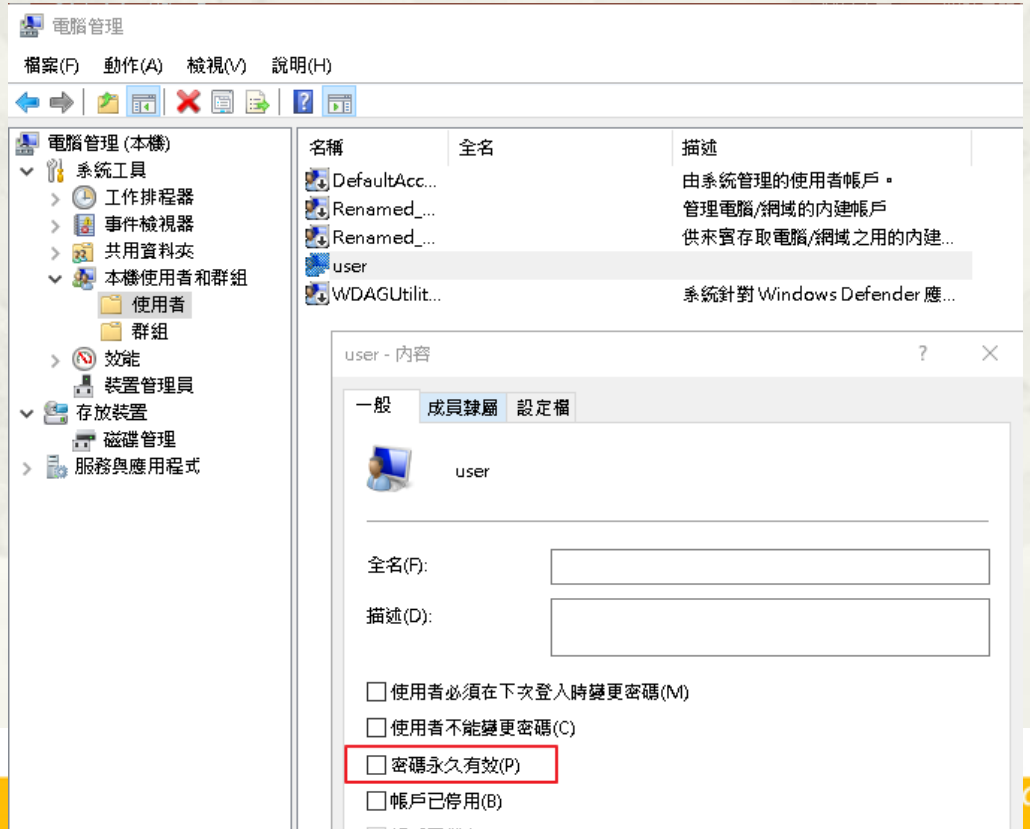
稽核時間	電腦名稱	網路	稽核結果	符合 / 不符合 / 排除	Log
2021-08-24 00:06:20	Mos-PC	140.112.3.76	NTUCC_20210823	466 / 15 / 99 (詳細資料)	檢視
2021-08-23 00:06:32	Mos-PC	140.112.3.76	NTUCC_20210807	468 / 15 / 97 (詳細資料)	檢視
2021-08-22 00:07:42	Mos-PC	140.112.3.76	NTUCC_20210807	468 / 15 / 97 (詳細資料)	檢視
2021-08-21 00:06:00	Mos-PC	140.112.3.76	NTUCC_20210807	468 / 15 / 97 (詳細資料)	檢視
2021-08-20 00:04:26	Mos-PC	140.112.3.76	NTUCC_20210807	483 / 0 / 97 (詳細資料)	檢視
2021-08-19 16:39:19	Mos-PC	140.112.3.76	NTUCC_20210807	483 / 0 / 97 (詳細資料)	檢視
2021-08-19 10:46:08	Mos-PC	140.112.3.76	政府組態基準	489 / 91 / 0 (詳細資料)	檢視
2021-08-19 00:05:02	Mos-PC	140.112.3.76	NTUCC_20210807	70 / 413 / 97 (詳細資料)	檢視
2021-08-18 00:03:16	Mos-PC	140.112.3.76	NTUCC_20210807	70 / 413 / 97 (詳細資料)	檢視
2021-08-17 00:02:11	Mos-PC	140.112.3.76	NTUCC_20210807	70 / 413 / 97 (詳細資料)	檢視

GCB 導入後

- 立即生效
  - Computer Settings > “互動式登入：不要顯示上次登入的使用者名稱”
    - 登入需自行輸入使用者名稱
- 非立即生效
  - Account Policy > “密碼必須符合複雜性需求”
    - 現階段舊密碼若不符合複雜密碼設置原則，且尚未超過最長使用期限，不會立即要求更改
- 可能無效(被其他設定 overwrite)
  - Account Policy > “密碼最長使用期限”
    - 會被個別使用者設定:"密碼永久有效" overwrite

“密碼永久有效“不應勾選

* 技服 GCB 未規範此欄位
  * 因為 gpedit.msc 無此設定
* Overwrite ”密碼最長使用期限”

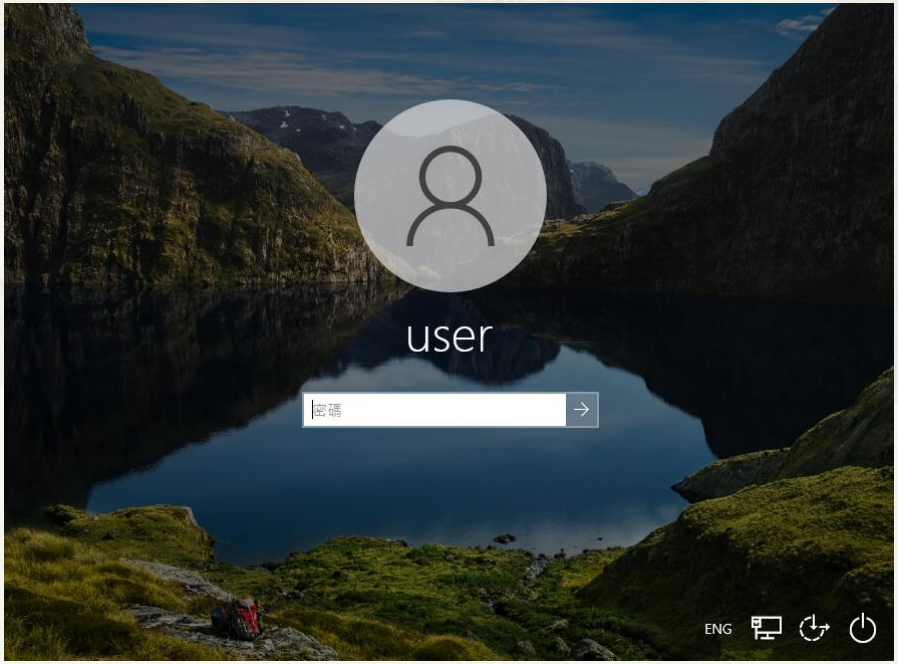


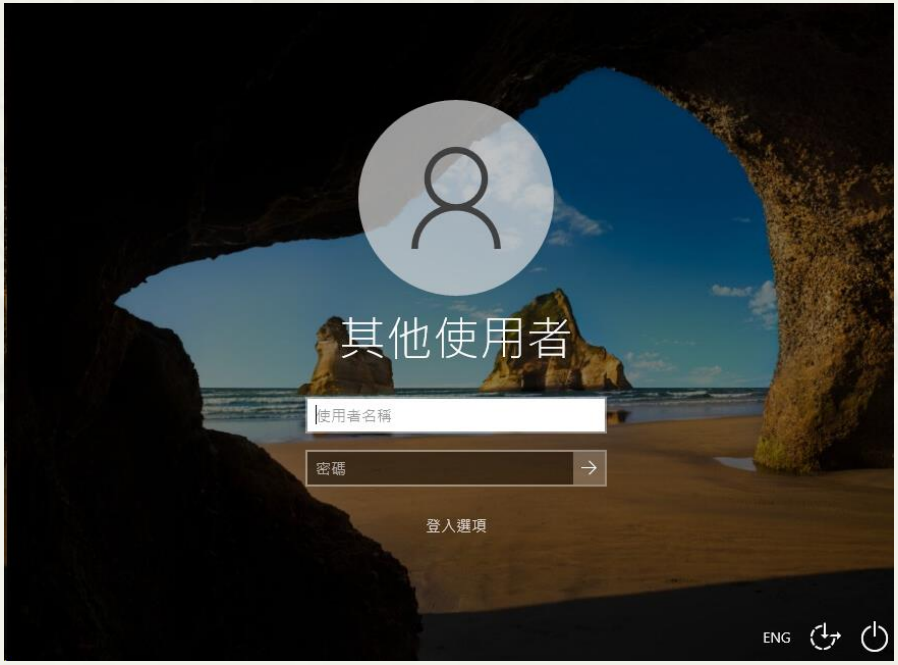
查詢密碼修改時間

* net user 帳號名稱

GCB 導入後
需自行輸入使用者名稱

* GCB 導入前
  * 預設自動帶出登入帳號
* GCB 導入後
  * 按 Ctrl+Alt+Del 才能登入
  * 需自行輸入登入帳號(請牢記)

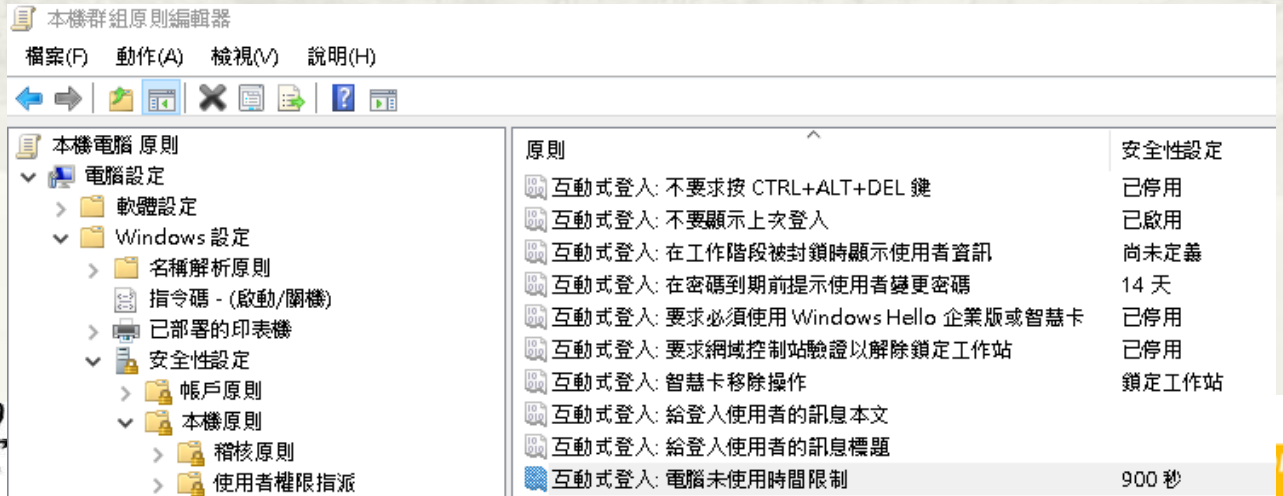




螢幕保護裝置逾時

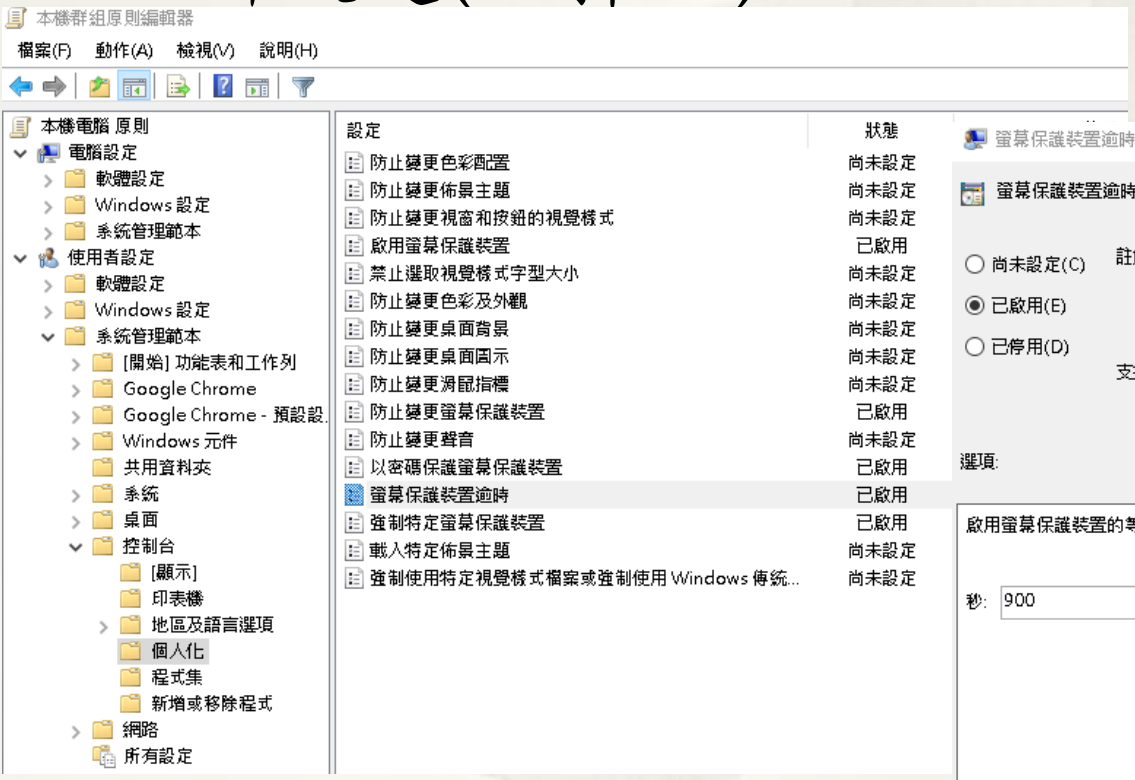
* 原始設定失效

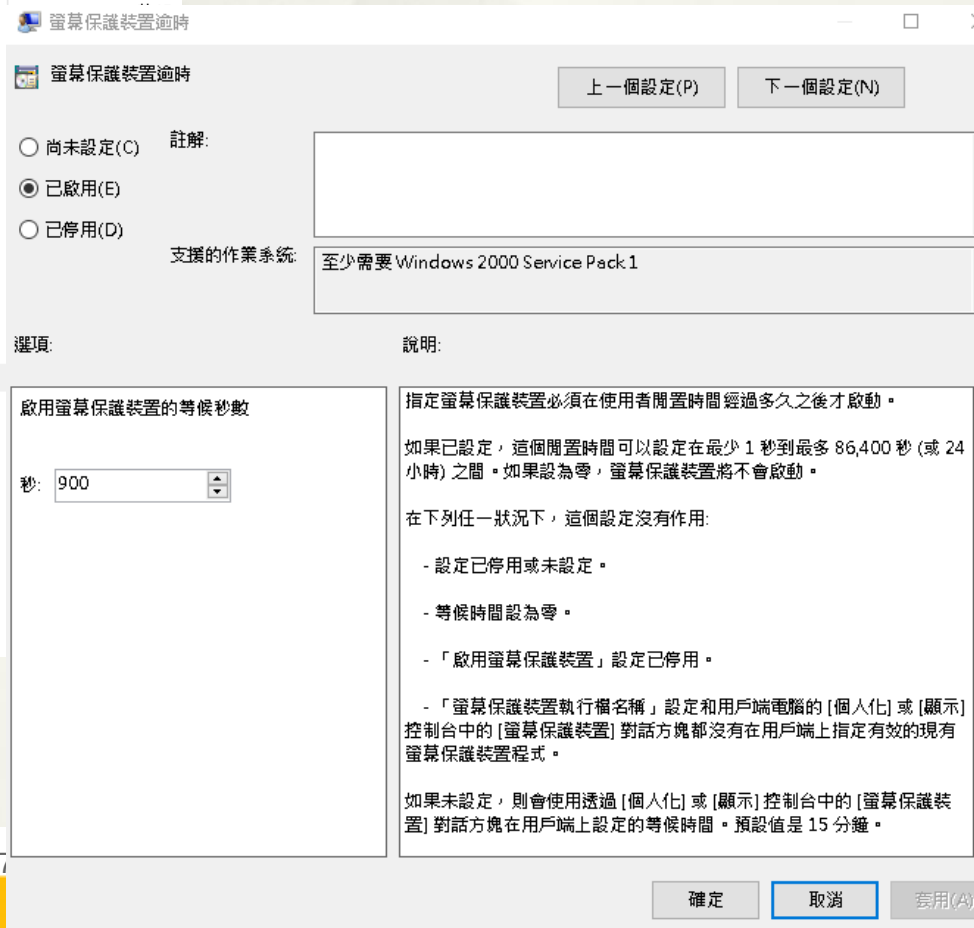
* 新設定(二擇一)



螢幕保護裝置逾時

* 新設定(二擇一)





GCB Windows10AccountSettings

項目	參數	值	說明
1	MinimumPasswordAge	1	密碼最短使用期限 1 天
2	MaximumPasswordAge	90	90 天內需變更一次密碼
3	MinimumPasswordLength	8	密碼長度最少應有8 個字元
4	PasswordComplexity	1	需符合複雜密碼設置原則
5	PasswordHistorySize	3	禁止重複使用最近 3 次相同密碼
6	LockoutBadCount	5	連續登入5 次錯誤後鎖定帳戶
7	ResetLockoutCount	15	連續登入錯誤之時間間隔為 15 分鐘
8	LockoutDuration	15	帳戶登入錯誤後之鎖定時間為 15分鐘
9	ClearTextPassword	0	不使用可還原的加密來存放密碼

複雜密碼設置原則

* 不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元
* 長度至少為6個字元.
  * 補充: 技服 GCB 規範至少8個字元
* 包含下列四種字元中的三種：
  * (1)英文大寫字元(A到Z)
  * (2)英文小寫字元(a到z)
  * (3)10進位數字(0到9)
  * (4)非英文字母字元(例如：!、$、#、%)

簡報完畢
謝謝