



# 政府組態基準(GCB)實作研習活動 Windows GCB部署說明與 實作練習

行政院國家資通安全會報技術服務中心

# 大綱

- 前言
- 群組原則介紹
- GCB導入流程
- 檢查GPO套用狀況之方式
- 恢復原始設定之方式
- 例外管理調整GCB設定值
- 實作練習

- 由於微軟Windows 7作業系統將於2020/1/14停止技術支援與軟體更新，為確保使用者電腦安全性，建議儘速升版至Windows 10作業系統
- 為協助機關於升版後可快速導入GCB，因此本課程採用Windows 10作業環境進行實作說明



The screenshot shows a Microsoft support page with the following content:

☰ Microsoft 🔍 🗑

## Windows 7 將於 2020 年 1 月 14 日終止支援

適用於：Windows 7

---

### Windows 7 支援週期

2009 年 10 月 22 日發行 Windows 7 時，Microsoft 已承諾為其提供 10 年的產品支援。當此 10 年期間結束時，Microsoft 將會停止對 Windows 7 的支援，以便將我們的投資集中於支援較新技術及絕佳新體驗。Windows 7 的明確終止支援日期定於 2020 年 1 月 14 日。在那之後，Windows Update 不再提供有助於保護您電腦的技術協助和軟體更新。Microsoft 極力建議您於 2020 年 1 月前擇時移轉至 Windows 10，以免發生您需要服務或支援卻無從取得的狀況。

# 群組原則介紹

A large, faint watermark of the NCCST logo is visible in the background, centered on the left side of the slide. It features the same shield emblem and the acronym "NCCST" in a light gray color.

NCCST

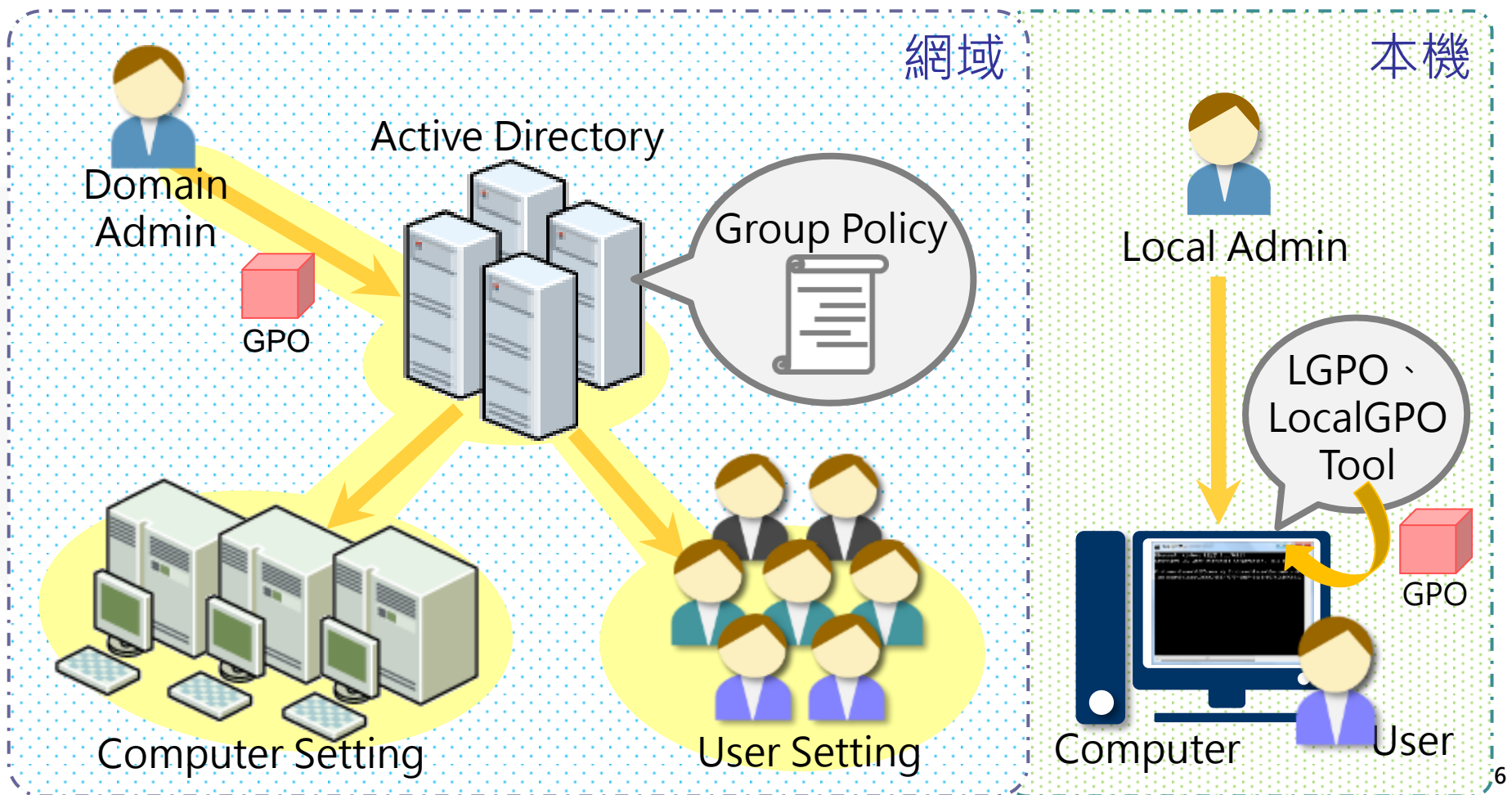
# 何謂群組原則(1/2)

- 群組原則：
  - 組織在電腦上強制套用設定的方式
- 目的：



# 何謂群組原則(2/2)

- 「群組原則物件」(GPO)是群組原則的集合
- 派送GPO的方式可分為網域與本機兩種環境





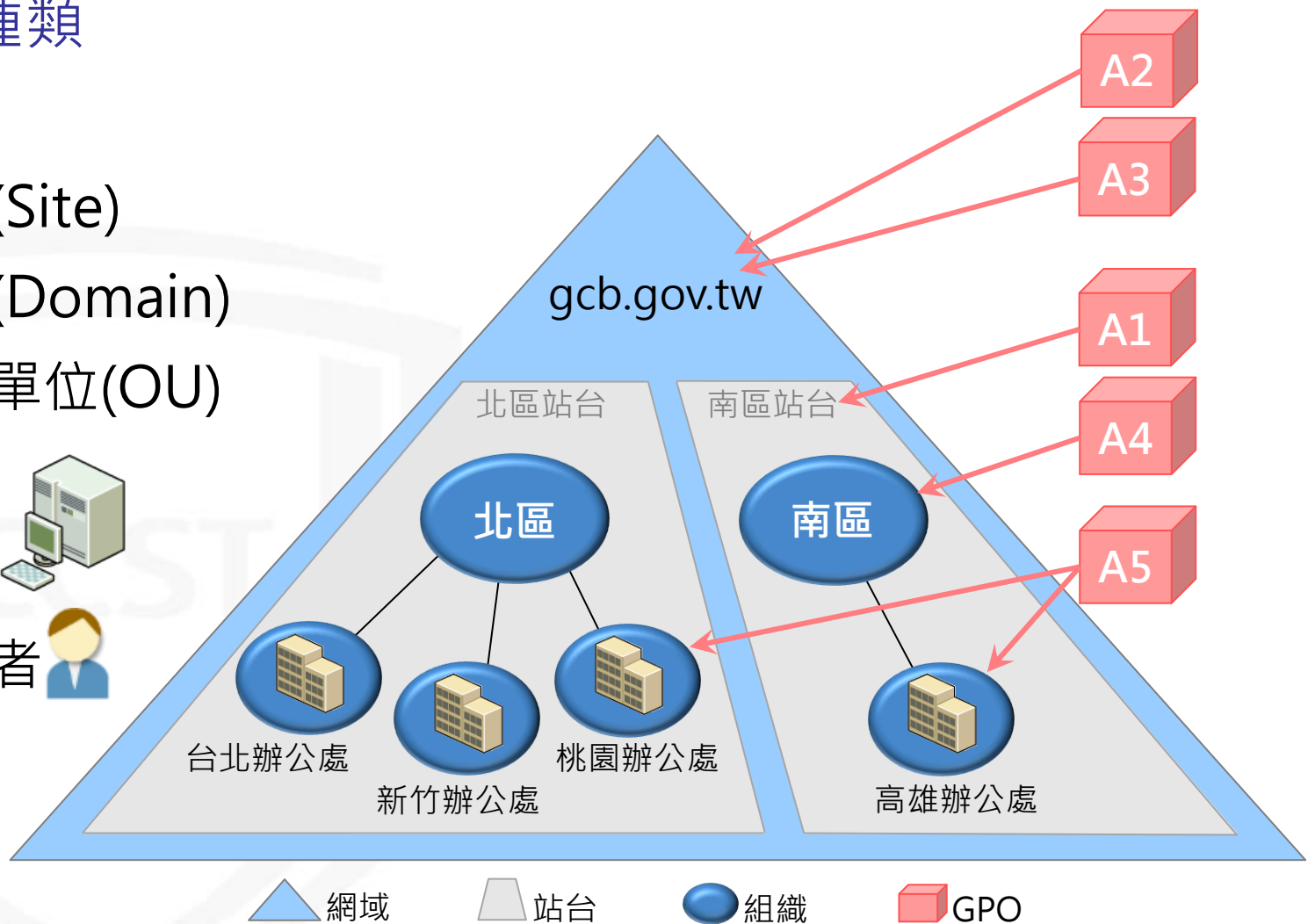
# 群組原則的關聯對象

- 連結種類

- 本機
- 站台(Site)
- 網域(Domain)
- 組織單位(OU)

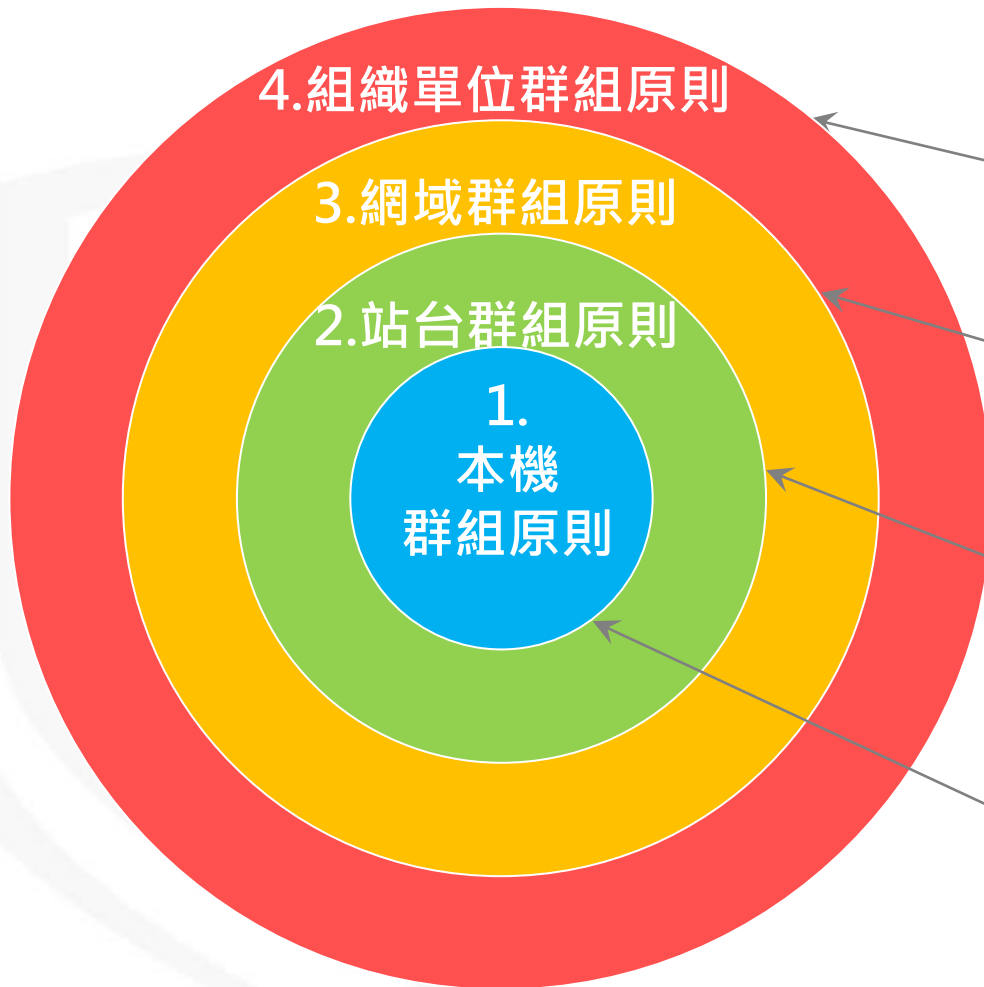
- 對象

- 電腦 
- 使用者 



# 群組原則的套用順序

到班時間=?    午休時間=?    下班時間=?



處長：

- 到班時間早上九點半

專委：

- 午休時間一個小時
- 下班時間下午五點半

高分：

- 午休時間一個半小時
- 下班時間下午五點半

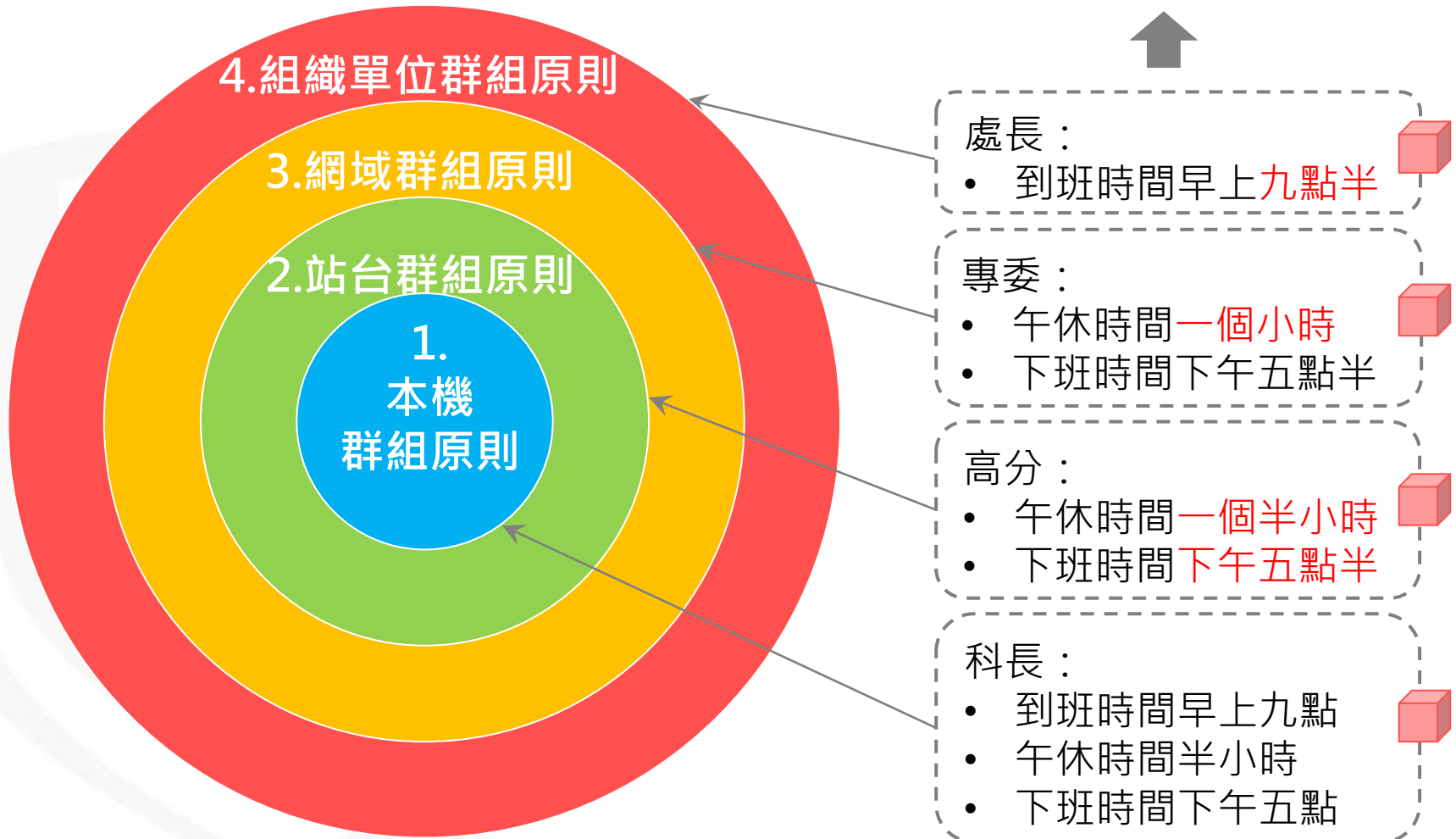
科長：

- 到班時間早上九點
- 午休時間半小時
- 下班時間下午五點



# 群組原則的套用順序

到班時間=9:30 午休時間=1HR 下班時間=17:30



# 群組原則的繼承型態



## 繼承 群組原則

- 下層**未**設定群組原則 ➔ 依循上層設定
- 下層**有**設定群組原則 ➔ 覆蓋上層設定

## 「禁止」繼承 原則



- 不繼承上層的群組原則



## 強制 (禁止覆蓋)

- 不允許下層的原則覆蓋上層的原則
- 應用在強制性的原則
- **GCB**群組原則建議使用強制避免被下層原則覆蓋

# 群組原則套用時機

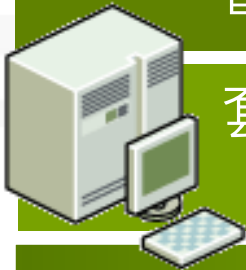
## GPO

內容  
組成

電腦設定

使用者設定

對象



套用於電腦的  
群組原則

套用於使用者的  
群組原則



衝突優  
先順序

電腦設定為主

更新  
機制

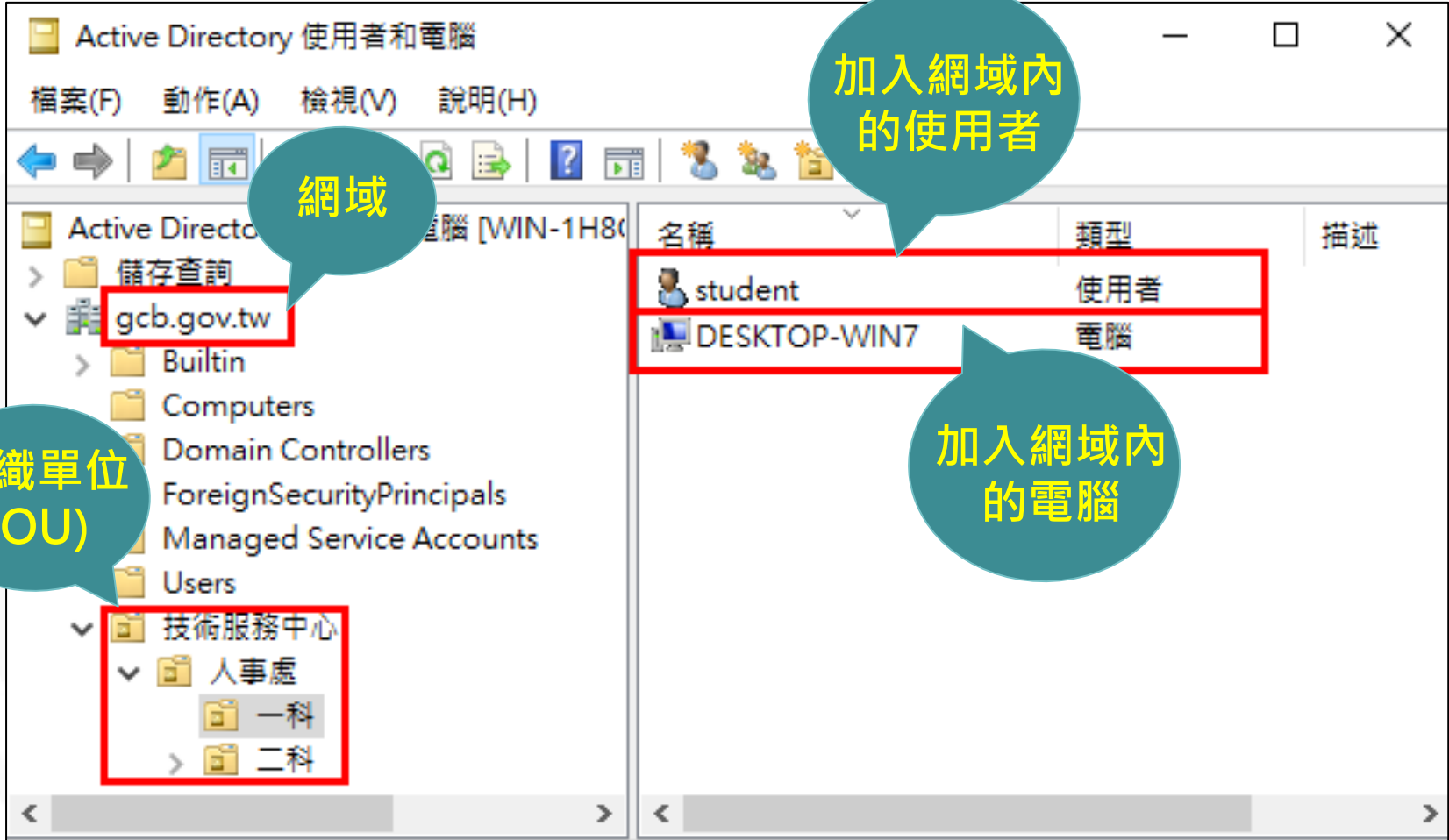
電腦下次開機時

使用者下次登入時

自動更新時間90~120分鐘

手動立即更新群組原則 `gpupdate /force`

# AD畫面說明



The screenshot shows the Active Directory console with the following callouts:

- 網域** (Domain): Points to the `gcb.gov.tw` domain in the left pane.
- 組織單位 (OU)** (Organizational Unit): Points to the `技術服務中心` (Technical Service Center) OU in the left pane.
- 加入網域內的使用者** (Users added to the domain): Points to the `student` user in the right pane.
- 加入網域內的電腦** (Computers added to the domain): Points to the `DESKTOP-WIN7` computer in the right pane.

名稱	類型	描述
student	使用者	
DESKTOP-WIN7	電腦	

# 群組原則的禁止繼承與強制(1/6)



主任室密碼到期提示時間=?

檢測評鑑組密碼到期提示時間=?

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：  
• 密碼到期**16**天前提示

技術服務中心：  
• 密碼到期**12**天前提示

主任室：  
• **未設定**密碼到期提示

檢測評鑑組：  
• 密碼到期**7**天前提示

# 群組原則的禁止繼承與強制(2/6)



主任室密碼到期提示時間=12天前

檢測評鑑組密碼到期提示時間=7天前

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：  
• 密碼到期**16**天前提示

技術服務中心：  
• 密碼到期**12**天前提示

主任室：  
• **未設定密碼到期提示**

檢測評鑑組：  
• 密碼到期**7**天前提示

# 群組原則的禁止繼承與強制(3/6)



主任室密碼到期提示時間=?

檢測評鑑組密碼到期提示時間=?

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：  
• 密碼到期**16**天前提示

技術服務中心：  
• 密碼到期**12**天前提示

主任室：**禁止繼承**  
• 未設定密碼到期提示

檢測評鑑組：  
• 密碼到期**7**天前提示

# 群組原則的禁止繼承與強制(4/6)



主任室密碼到期提示時間=無

檢測評鑑組密碼到期提示時間=7天前

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：  
• 密碼到期**16**天前提示

技術服務中心：  
• 密碼到期**12**天前提示

主任室：**禁止繼承**  
• 未設定密碼到期提示

檢測評鑑組：  
• 密碼到期**7**天前提示



# 群組原則的禁止繼承與強制(5/6)



主任室密碼到期提示時間=?

檢測評鑑組密碼到期提示時間=?

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：**強制**

- 密碼到期**16**天前提示

技術服務中心：

- 密碼到期**12**天前提示

主任室：**禁止繼承**

- 未設定密碼到期提示

檢測評鑑組：

- 密碼到期**7**天前提示

# 群組原則的禁止繼承與強制(6/6)



主任室密碼到期提示時間=16天前

檢測評鑑組密碼到期提示時間=16天前

套用順序

站台群組原則

網域群組原則

上層組織單位群組原則

下層組織單位群組原則



gcb.gov.tw網域：**強制**

- 密碼到期16天前提示

技術服務中心：

- 密碼到期12天前提示

主任室：**禁止繼承**

- 未設定密碼到期提示

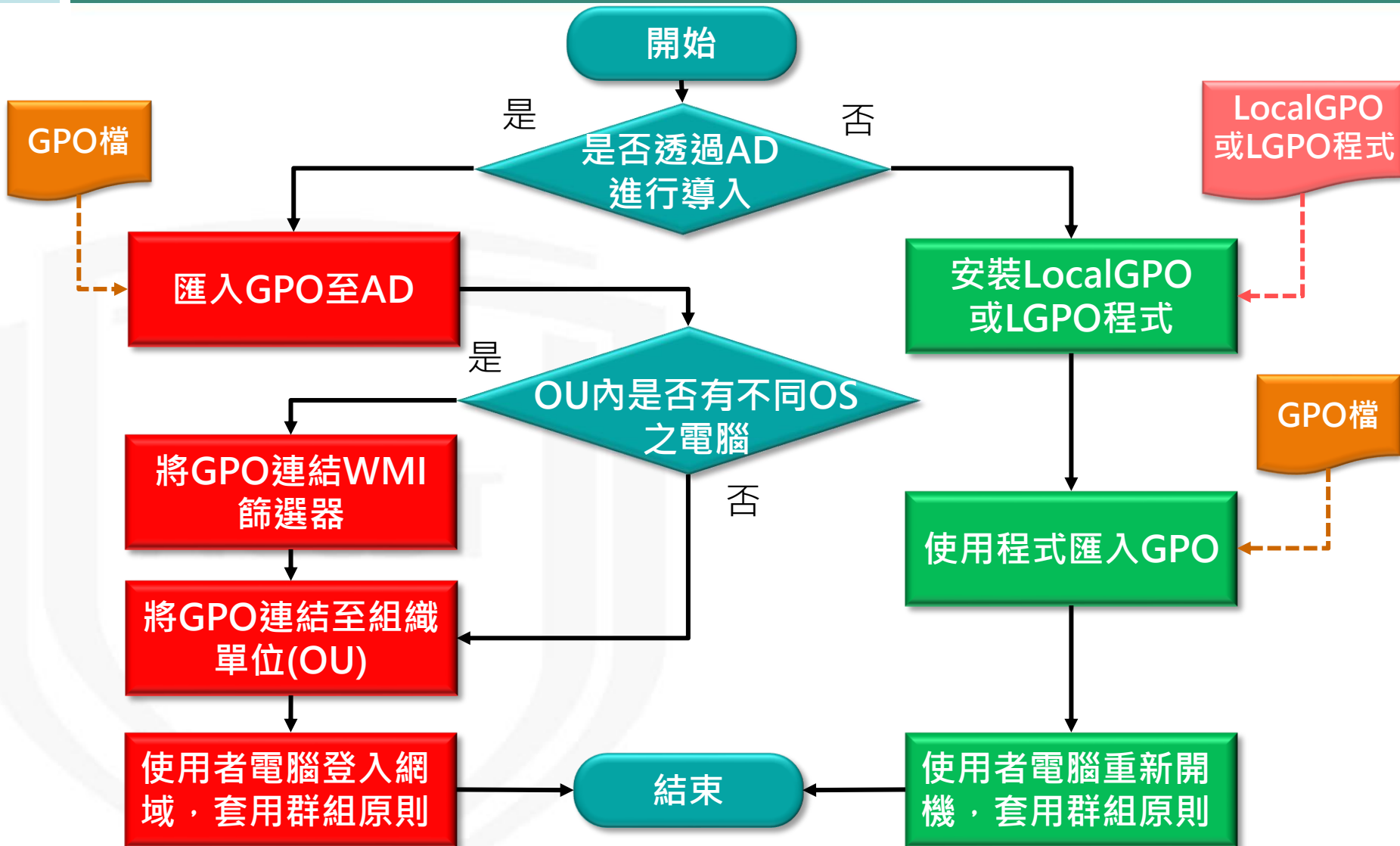
檢測評鑑組：

- 密碼到期7天前提示

# GCB導入流程

NCCST

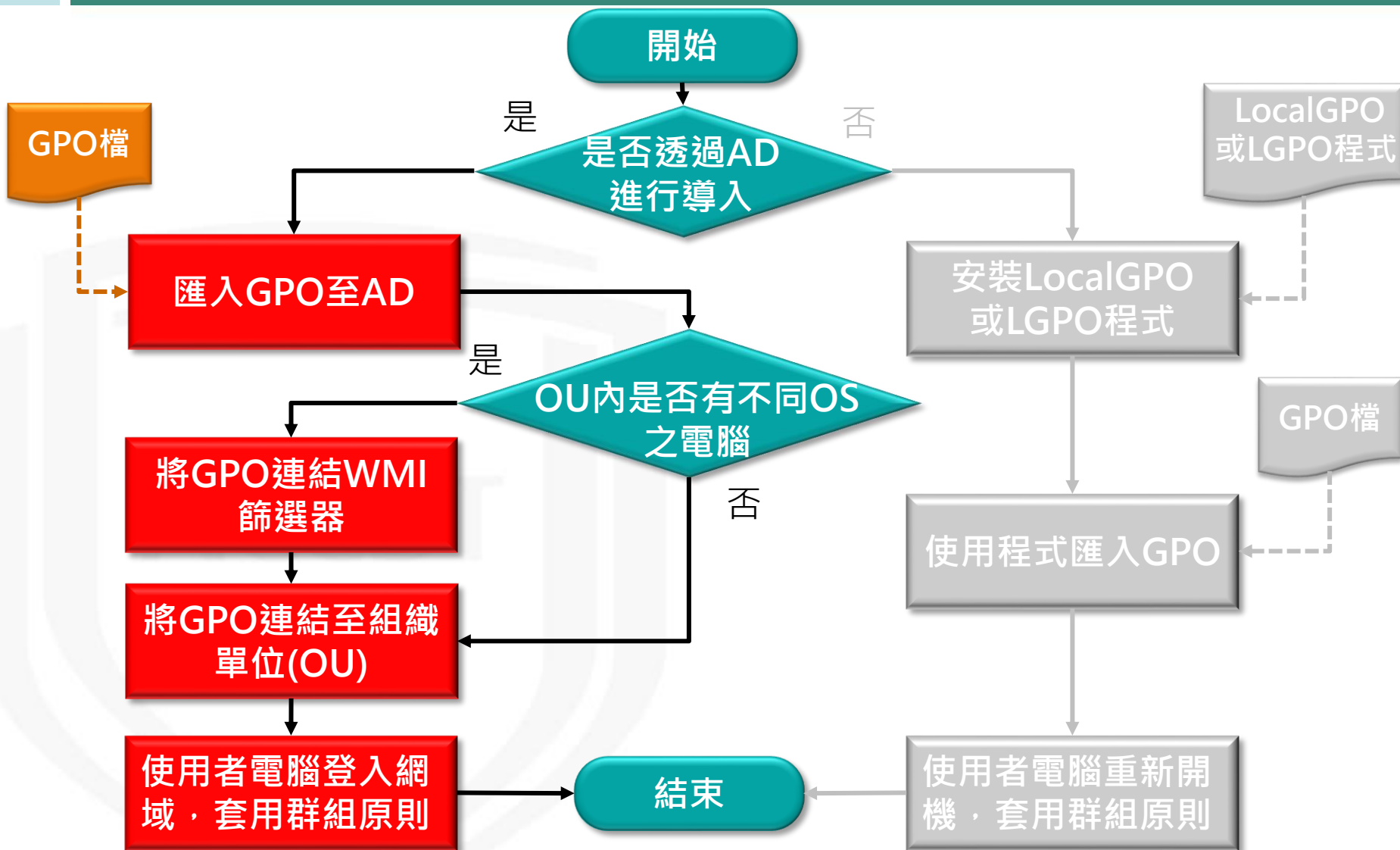
# GCB導入流程



# 使用AD導入GCB

NCCST

# GCB導入流程



# 匯入GPO至AD(1/4)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理
- 步驟3：在群組原則物件節點按滑鼠右鍵
- 步驟4：點選「新增」
- 步驟5：在「名稱」欄位輸入群組原則物件的名稱
- 步驟6：點選「確定」按鈕



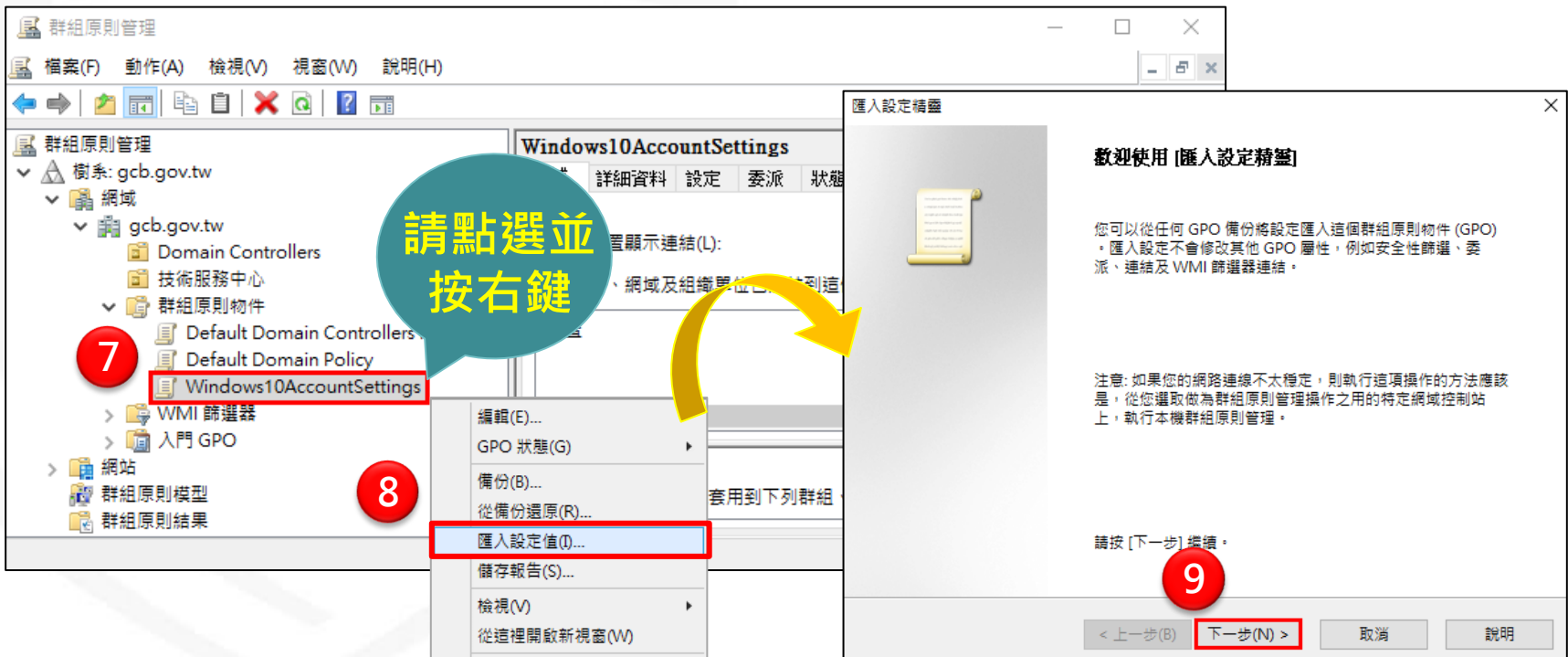
The screenshot illustrates the process of adding a new Group Policy Object (GPO) in Windows. It is divided into six numbered steps:

- Step 1:** The Windows Start menu is shown with the 'System Management Tools' folder highlighted.
- Step 2:** The 'Group Policy Management' application is selected from the Start menu.
- Step 3:** In the Group Policy Management console, the 'Group Policy Objects' folder under the 'gcb.gov.tw' domain is selected.
- Step 4:** A right-click context menu is opened over the 'Group Policy Objects' folder, and the 'New' option is selected.
- Step 5:** The 'New GPO' dialog box is shown with the name 'Windows10AccountSettings' entered in the 'Name' field.
- Step 6:** The 'OK' button in the 'New GPO' dialog box is clicked to confirm the creation.

A callout bubble in the center of the console window says: **請點選並按右鍵** (Please click and right-click).

# 匯入GPO至AD(2/4)

- 步驟7：點選新建的群組原則物件按滑鼠**右鍵**
- 步驟8：選擇「匯入設定值」
- 步驟9：在歡迎使用【匯入設定精靈】頁面，點選「**下一步**」按鈕



群組原則管理

檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)

群組原則管理

樹系: gcb.gov.tw

網路

gcb.gov.tw

Domain Controllers

技術服務中心

群組原則物件

Default Domain Controllers

Default Domain Policy

Windows10AccountSettings

WMI 篩選器

入門 GPO

網站

群組原則模型

群組原則結果

Windows10AccountSettings

詳細資料 設定 委派 狀態

顯示連結(L):

、網路及組織單位已

套用到下列群組

編輯(E)...

GPO 狀態(G)

備份(B)...

從備份還原(R)...

匯入設定值(I)...

儲存報告(S)...

檢視(V)

從這裡開啟新視窗(W)

匯入設定精靈

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，例如安全性篩選、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，從您選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。

< 上一步(B) **下一步(N) >** 取消 說明

請點選並按右鍵

7

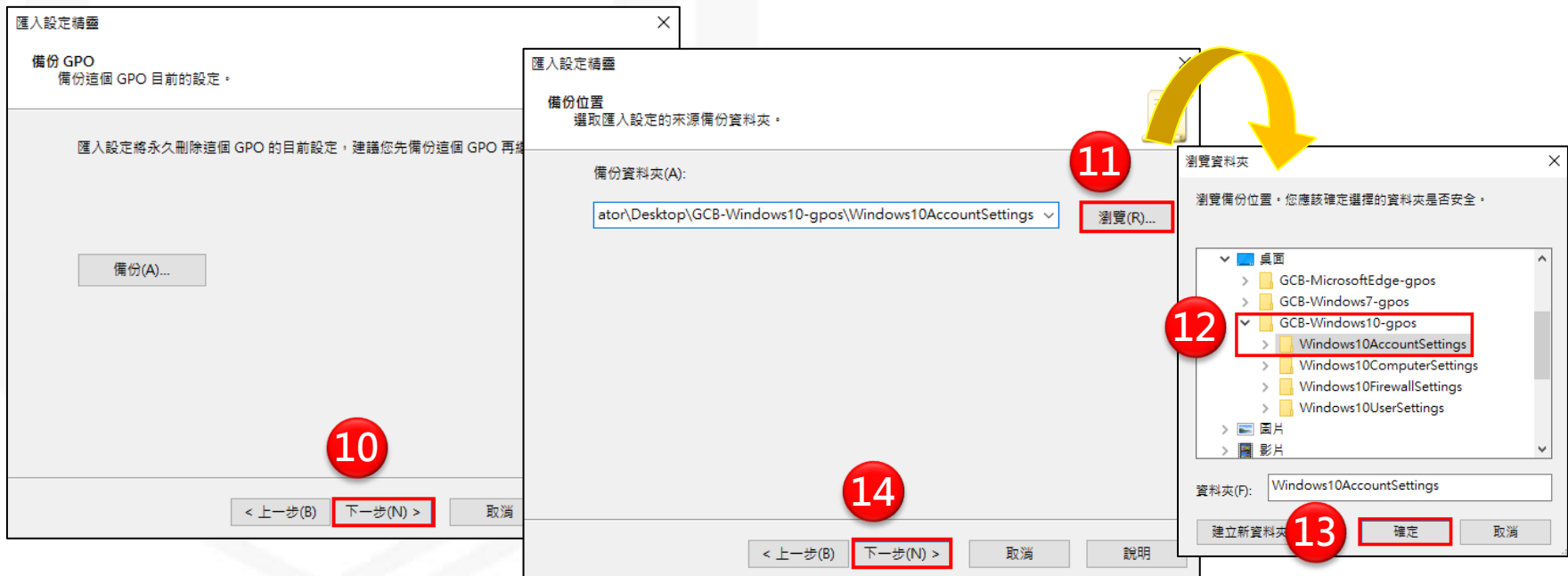
8

9



# 匯入GPO至AD(3/4)

- 步驟10：在備份GPO頁面，點選「下一步」按鈕
- 步驟11：在備份位置頁面，點選「瀏覽」按鈕
- 步驟12：點選欲匯入的GPO資料夾
- 步驟13：點選「確定」按鈕
- 步驟14：在備份位置頁面，點選「下一步」按鈕



# 匯入GPO至AD(4/4)

- 步驟15：在來源GPO頁面，點選「下一步」按鈕
- 步驟16：在掃描備份頁面，點選「下一步」按鈕
- 步驟17：在正在完成匯入設定頁面，點選「完成」按鈕
- 步驟18：在匯入進度頁面，點選「確定」按鈕，完成匯入GPO至群組原則物件中



The image displays four sequential screenshots of the Group Policy Migration Wizard, illustrating the final steps of the process:

- Step 15:** The 'Source GPO' screen shows a list of backup GPOs. The 'Next Step' button is highlighted with a red box and a red circle labeled '15'.
- Step 16:** The 'Scan Backup' screen shows the results of scanning the backup. The 'Next Step' button is highlighted with a red box and a red circle labeled '16'.
- Step 17:** The 'Completing Migration Settings' screen shows a summary of the migration. The 'Finish' button is highlighted with a red box and a red circle labeled '17'.
- Step 18:** The 'Migration Progress' screen shows the migration is complete. A large blue callout bubble with the text '顯示匯入成功' (Display Migration Success) is overlaid on the screen. The 'OK' button is highlighted with a red box and a red circle labeled '18'.

# 將GPO連結WMI篩選器(1/4)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理
- 步驟3：在WMI篩選器節點按滑鼠右鍵
- 步驟4：點選「新增」
- 步驟5：在新增WMI篩選器視窗，「名稱」欄位輸入WMI篩選器名稱
- 步驟6：點選「新增」按鈕



請點選並按右鍵

1 Windows 系統管理工具

2 群組原則管理

3 WMI 篩選器

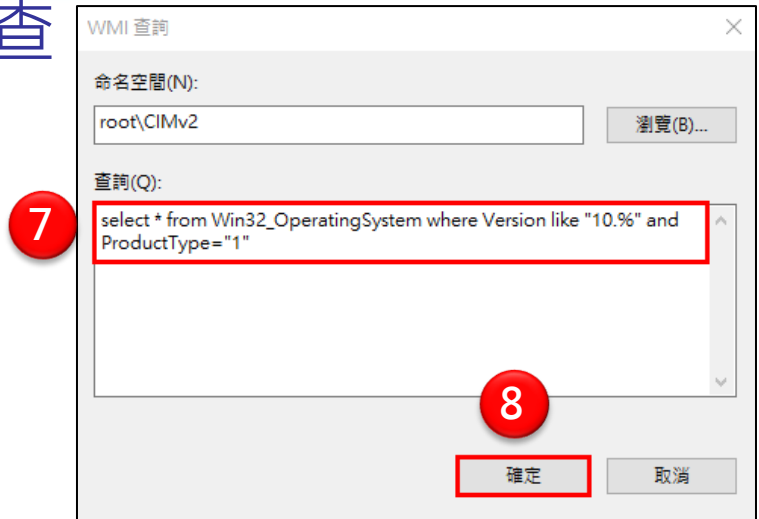
4 新增(N)...

5 名稱(N): Windows10篩選器

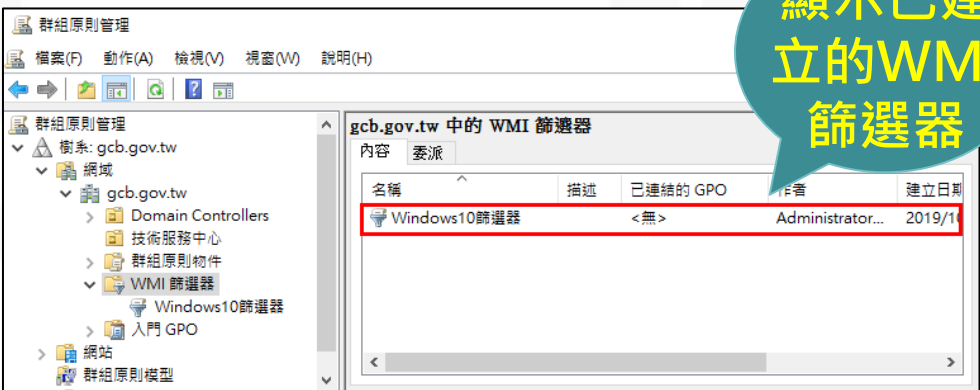
6 新增(A)

# 將GPO連結WMI篩選器(2/4)

- 步驟7：在WMI查詢視窗，「查詢」欄位輸入select \* from Win32\_OperatingSystem where Version like "10.%" and ProductType="1"
- 步驟8：點選「確定」按鈕
- 步驟9：在新增WMI篩選器視窗，點選「儲存」按鈕，完成建立WMI篩選器



顯示已建立的WMI篩選器



# 將GPO連結WMI篩選器(3/4)

- 步驟10：點選Windows10 GPO
- 步驟11：於「領域」標籤頁面移至最後，指定WMI篩選器
- 步驟12：點選「是」，將WMI篩選器連結至GPO



請選擇要連結的GPO

請選擇要連結的WMI篩選器

1個GPO只能指定1個WMI篩選器，當符合該WMI篩選器所設定的OS版本號與ProductType參數就會套用該GPO

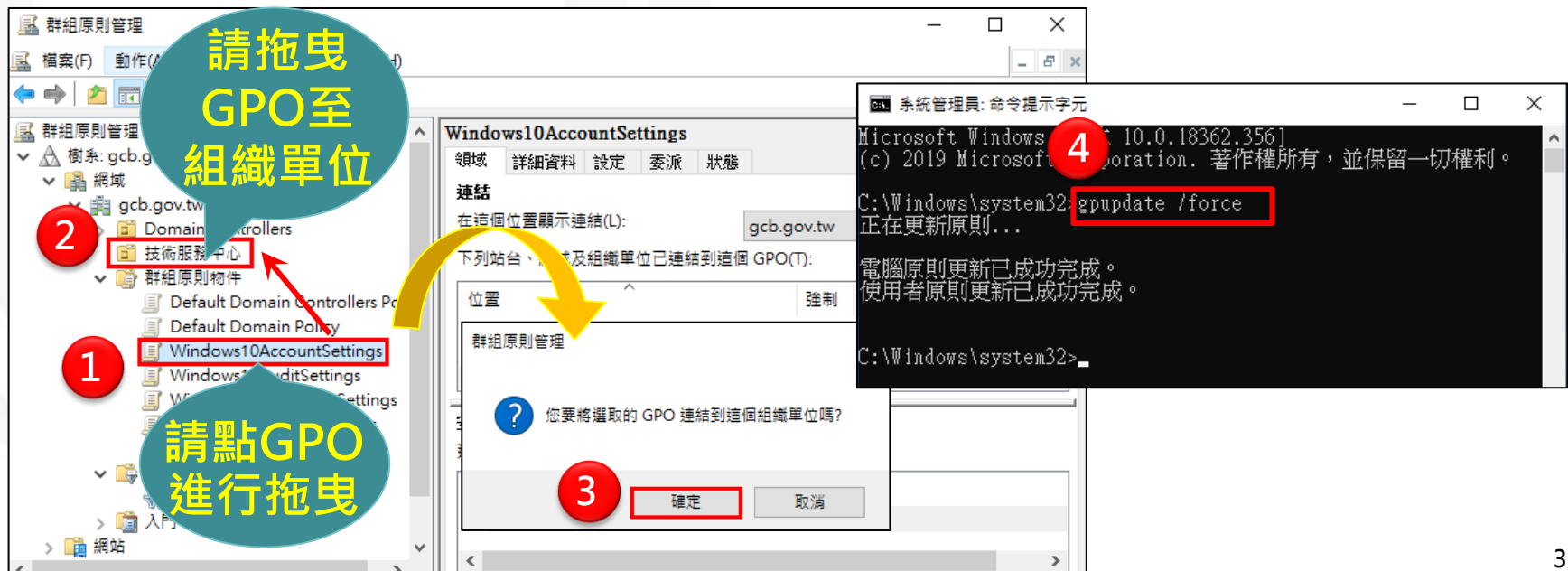
# 將GPO連結WMI篩選器(4/4)



- 再次執行前述1 ~ 11的步驟建立Windows 7的WMI篩選器
- Windows 7 與Windows 10 WMI篩選器語法
  - Windows 7 WMI篩選器：select \* from Win32\_OperatingSystem where Version like "6.1%" and ProductType="1"
  - Windows 10 WMI篩選器：select \* from Win32\_OperatingSystem where Version like "10.%" and ProductType="1"
- 語法說明：
  - Windows 7與Windows Server 2008 R2的版本號為6.1
  - Windows 10與Windows Server 2016的版本號為10.0
  - 因Windows OS與Windows Server OS有共用版本號的狀況，需要使用ProductType此參數來輔助辨認
    - Windows OS的ProductType = "1"
    - Windows Server OS(網域控制站)的ProductType = "2"
    - Windows Server OS(非網域控制站)的ProductType = "3"

# 將GPO連結至組織單位(OU)

- 步驟1：點選已匯入GPO的群組原則物件
- 步驟2：拖曳至組織單位(OU)
- 步驟3：點選「確定」按鈕，完成GPO連結至組織單位
- 步驟4：使用者電腦重新開機或使用gpupdate /force 指令更新群組原則，即可套用GCB設定



The screenshot illustrates the process of linking a Group Policy Object (GPO) to an Organizational Unit (OU) and updating it. It consists of three main parts:

- Group Policy Management Console:** Shows the hierarchy of Group Policy Objects (GPOs) under the domain `gcb.gov.tw`. The GPO `Windows10AccountSettings` is selected (Step 1). A yellow arrow indicates it is being dragged to the `技術服務中心` (Technical Service Center) OU (Step 2).
- Confirmation Dialog:** A dialog box asks, "您要將選取的 GPO 連結到這個組織單位嗎?" (Do you want to link the selected GPO to this organizational unit?). The `確定` (OK) button is highlighted (Step 3).
- Command Prompt:** A terminal window shows the command `gpupdate /force` being executed (Step 4). The output indicates that the computer policy update was successful.

Annotations in the image include:

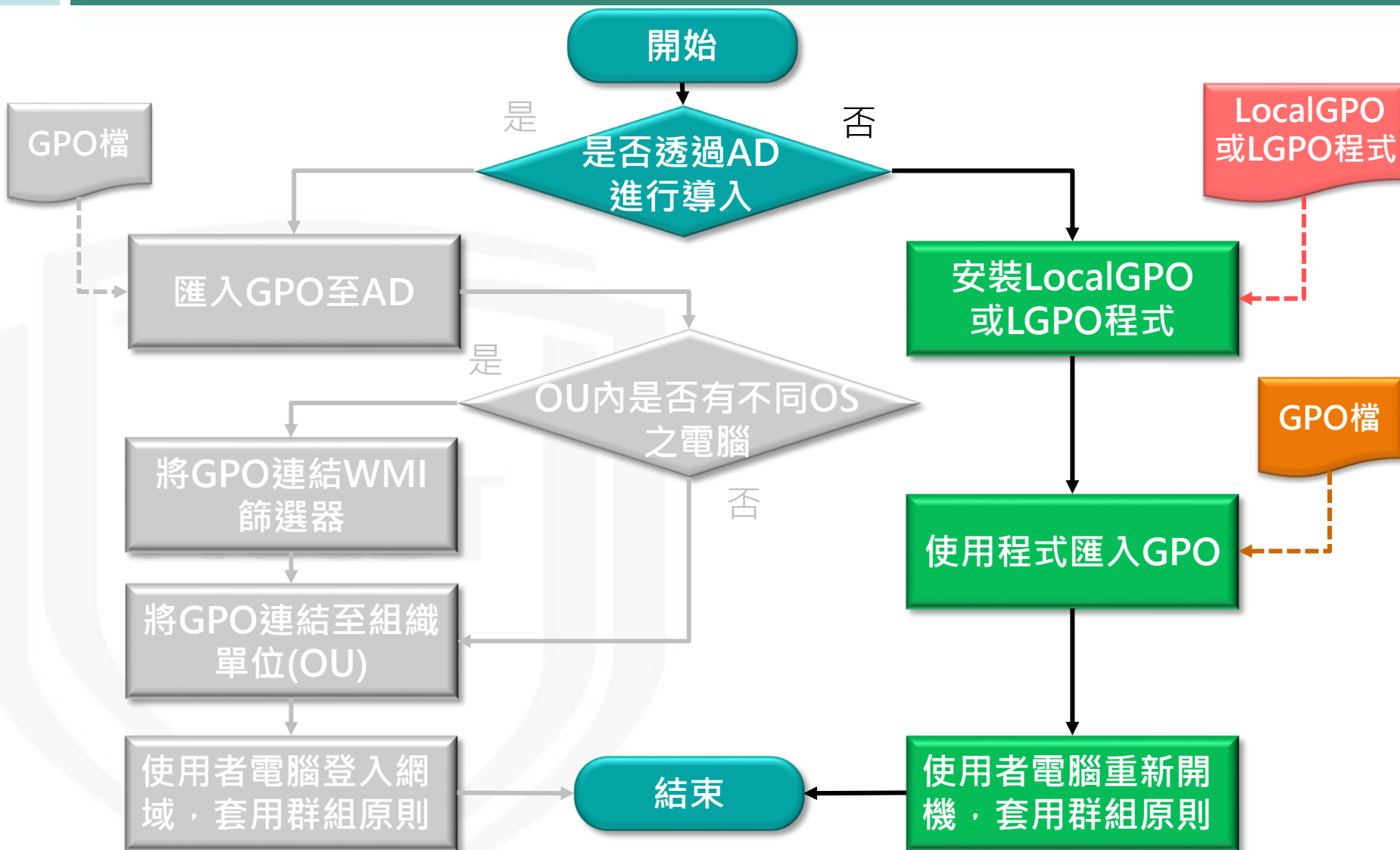
- Red circles with numbers 1, 2, 3, and 4 corresponding to the steps.
- Yellow callouts: "請拖曳 GPO 至 組織單位" (Please drag GPO to organizational unit) and "請點 GPO 進行拖曳" (Please click GPO for dragging).
- Red boxes highlighting the GPO name, the OU name, the OK button, and the command.

# 使用單機導入GCB

NCCST



# GCB導入流程

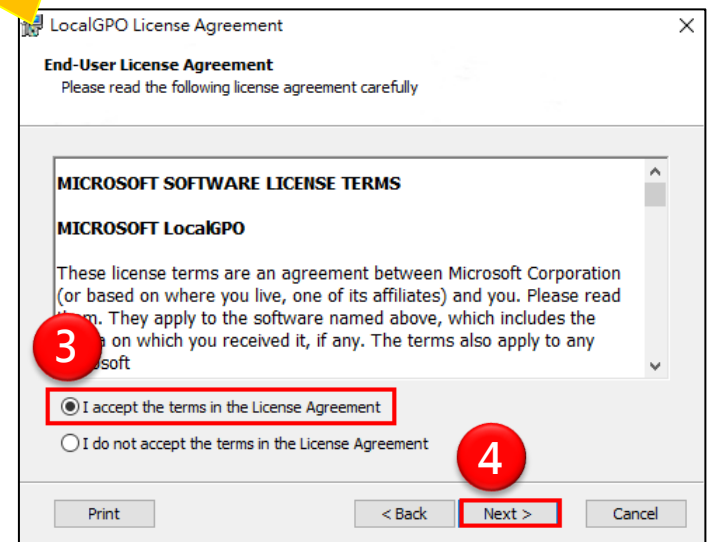
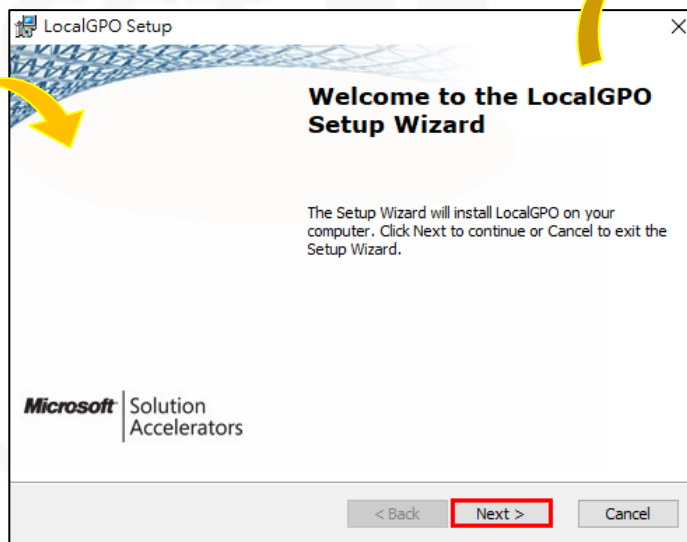


# 使用LocalGPO程式導入GCB

NCCST

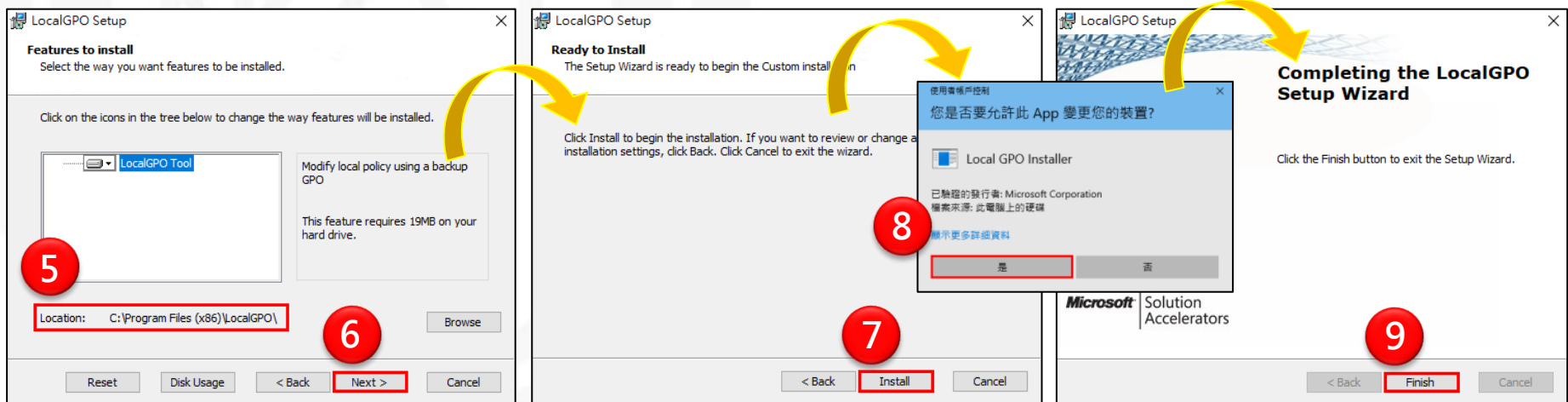
# 安裝LocalGPO程式(1/2)

- 步驟1：執行「LocalGPO」安裝檔
- 步驟2：在Welcome to the LocalGPO Setup Wizard 頁面，點選「Next」按鈕
- 步驟3：在End-User License Agreement頁面，勾選接受授權協議
- 步驟4：在End-User License Agreement頁面，點選「Next」按鈕



# 安裝LocalGPO程式(2/2)

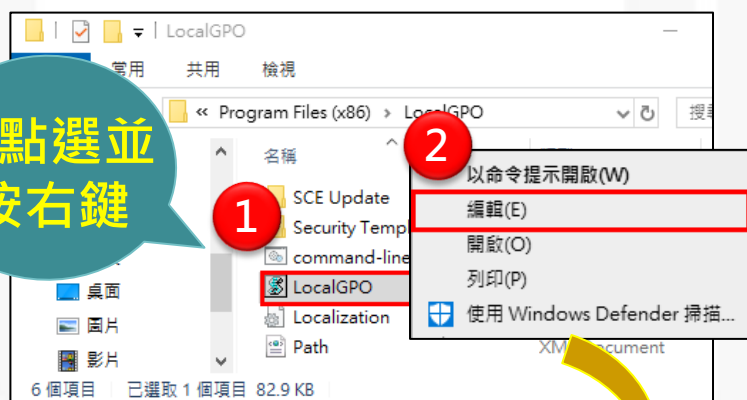
- 步驟5：在Features to Install頁面，確認安裝路徑
- 步驟6：在Features to Install頁面，點選「Next」按鈕
- 步驟7：在Ready to Install頁面，點選「Install」按鈕，進行安裝
- 步驟8：在使用者帳戶控制頁面，點選「是」按鈕
- 步驟9：在Completing the LocalGPO Setup Wizard頁面，點選「Finish」按鈕，完成安裝作業



# 調整LocalGPO設定檔(1/2)

- 步驟1：開啟LocalGPO資料夾(C:\Program Files (x86)\LocalGPO)→點選「LocalGPO.wsf」按滑鼠**右鍵**
- 步驟2：點選「編輯」
- 步驟3：搜尋「Sub ChkOSVersion」找到下圖程式碼位置

請點選並  
按右鍵



1

2



搜尋  
關鍵字

```
'Checks whether the operating system is Windows XP or _
'Windows Server 2003 or Windows Vista or Windows Server 2008 or _
'Windows 7 or Windows Server 2008 R2 or Windows 8 or Windows Server 8

If(Left(strOpVer,3) = "6.2") and (strProductType <> "1") then
    strOS = "WS12"
ElseIf(Left(strOpVer,3) = "6.2") and (strProductType = "1") then
    strOS = "Win8"
ElseIf(Left(strOpVer,3) = "6.1") and (strProductType <> "1") then
    strOS = "WS08R2"
ElseIf(Left(strOpVer,3) = "6.1") and (strProductType = "1") then
    strOS = "Win7"
ElseIf(Left(strOpVer,3) = "6.0") and (strProductType <> "1") then
    strOS = "WS08"
ElseIf(Left(strOpVer,3) = "6.0") and (strProductType = "1") then
    strOS = "VISTA"
ElseIf(Left(strOpVer,3) = "5.2") and (strProductType <> "1") then
    strOS = "WS03"
ElseIf(Left(strOpVer,3) = "5.2") and (strProductType = "1") then
    strOS = "XP"
ElseIf(Left(strOpVer,3) = "5.1") and (strProductType = "1") then
    strOS = "XP"
Else
    strMessage = DisplayMessage(conLABEL_CODE002)
    Call MsgBox(strMessage, vbOKOnly + vbCritical, strTitle)
    Call CleanupandExit
End If
```

找到此段  
程式碼

# 調整LocalGPO設定檔(2/2)

- 步驟4：將程式碼更改為以下內容後存檔

```
'Checks whether the operating system is Windows XP or _  
'Windows Server 2003 or Windows Vista or Windows Server 2008 or _  
4 Windows 7 or Windows Server 2008 R2 or Windows 8 or Windows Server 8
```

```
If(Left(strOpVer,3) = "10.") and (strProductType = "1") then  
    strOS = "Win8"  
Elseif(Left(strOpVer,3) = "6.2") and (strProductType <> "1") then  
    strOS = "WS12"
```

```
Elseif(Left(strOpVer,3) = "6.2") and (strProductType = "1") then  
    strOS = "Win8"  
Elseif(Left(strOpVer,3) = "6.1") and (strProductType <> "1") then  
    strOS = "WS08R2"
```

```
Elseif(Le  
    strOS
```

```
Elseif(Le  
    strOS
```

```
Elseif(Le  
    strOS
```

```
Elseif(Le  
    strOS
```

```
Elseif(Le  
    strOS
```

```
Elseif(Le  
    strOS
```

```
Else
```

```
    strMessage = DisplayMessage(conLABEL_CODE002)  
    Call MsgBox(strMessage, vbOKOnly + vbCritical, strTitle)  
    Call CleanupandExit  
End If
```

- 修改說明：

- 新增第一行程式碼

**If(Left(strOpVer,3) = "10.") and (strProductType = "1") then  
strOS = " Win8 "**

- 調整第二行程式碼

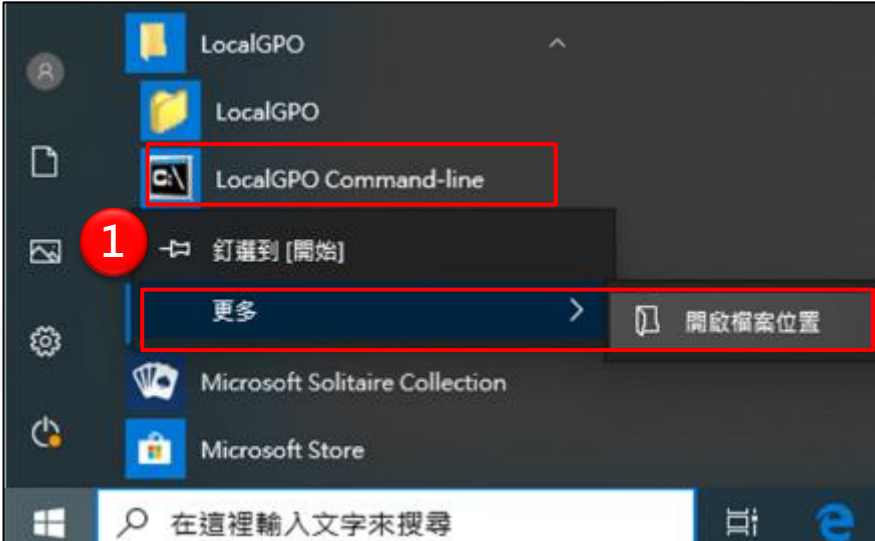
**Elseif(Left(strOpVer,3) = "6.2") and (strProductType <> "1") then  
strOS = "WS12"**

請依紅字  
標示修改

# 使用LocalGPO程式匯入GPO(1/2)



- 步驟1：點擊開始→LocalGPO資料夾→點選「LocalGPO Command-line」按滑鼠右鍵→更多→開啟檔案位置
- 步驟2：點選「LocalGPO Command-line」按滑鼠右鍵
- 步驟3：選擇「以系統管理員身分執行」



# 使用LocalGPO程式匯入GPO(2/2)



- 步驟4：複製欲匯入的GPO完整目錄路徑
- 步驟5：於「LocalGPO Command-line」輸入 `cscript LocalGPO.wsf /path:<GPO完整目錄路徑>`
- 步驟6：電腦重新開機或使用 `gpupdate /force` 指令更新組態

The screenshot shows two windows. The top window is Windows Explorer with the address bar containing the path `ws10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}`. A red circle with the number '4' is next to the address bar. A callout bubble says '請複製 GPO 完整路徑'. The bottom window is '系統管理員: LocalGPO Command-line'. It shows the command `cscript LocalGPO.wsf /path:C:\Users\student\Desktop\GCB-Windows10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}` being entered. A red circle with the number '5' is next to the command. A callout bubble says '請輸入 匯入GPO 語法'. Below that, the output shows 'Local Policy Modified!' and 'Please restart the computer to refresh the Local Policy'. A second callout bubble says '顯示修改 成功'. At the bottom, the command `gpupdate /force` is entered, with a red circle with the number '6' next to it.

路徑不能  
有空白

請輸入  
匯入GPO  
語法

請複製  
GPO  
完整路徑

顯示修改  
成功

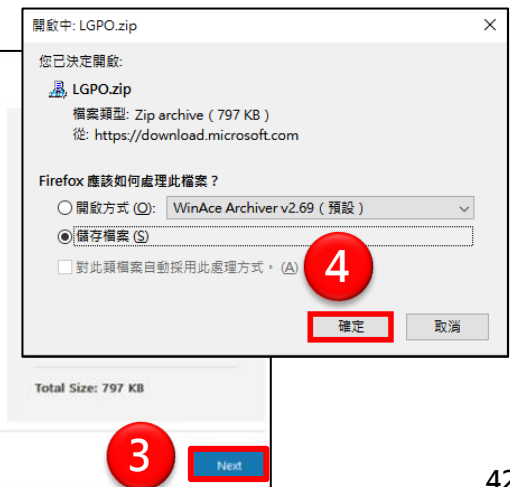
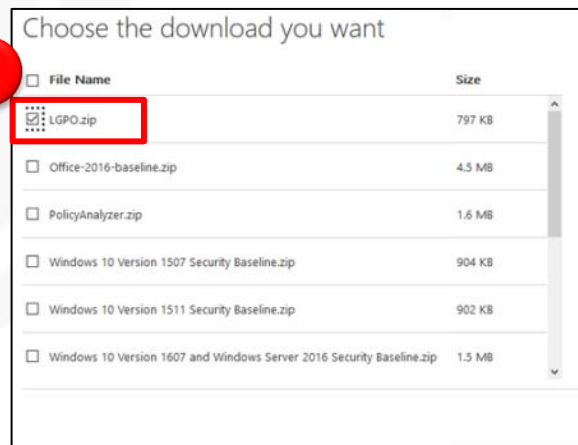


# 使用LGPO程式導入GCB

NCCST

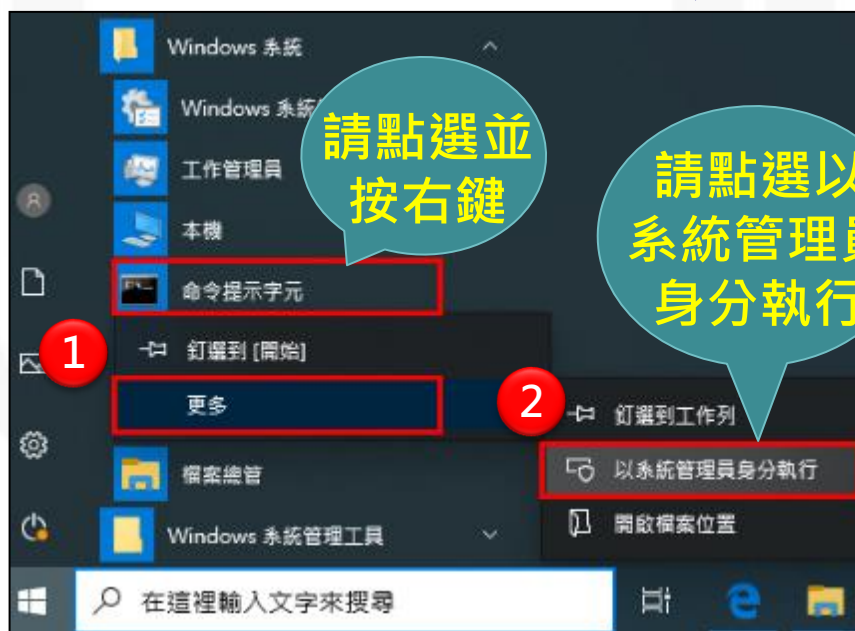
# 下載LGPO程式

- 步驟1：至<https://www.microsoft.com/en-us/download/details.aspx?id=55319>，點選「Download」按鈕，下載LGPO程式
- 步驟2：在Choose the download you want頁面，勾選「LGPO.zip」
- 步驟3：在Choose the download you want頁面，點選「Next」按鈕
- 步驟4：儲存檔案，點選「確定」按鈕



# 使用LGPO程式匯入GPO(1/3)

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
- 步驟2：**選擇「以系統管理員身分執行」**
- 步驟3：複製LGPO應用程式解壓縮後的完整目錄路徑
- 步驟4：於「命令提示字元」輸入cd <LGPO應用程式完整目錄路徑>，切換至LGPO目錄



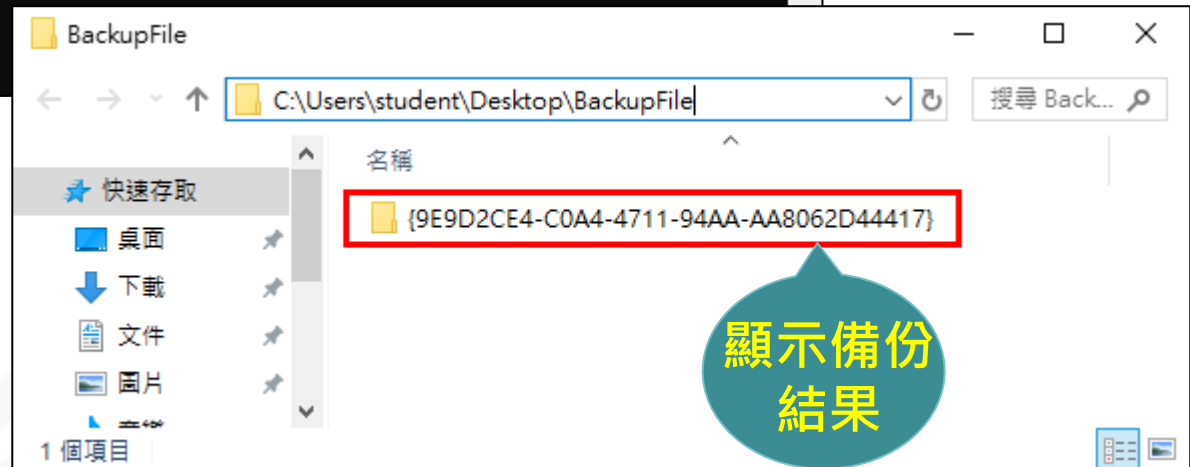
# 使用LGPO程式匯入GPO(2/3)

- 步驟5：於「命令提示字元」輸入指令  
**LGPO.exe /b <絕對路徑>**，備份電腦當下組態設定

```
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\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}"  
C:\Users\student\Desktop\
```

請輸入  
備份語法

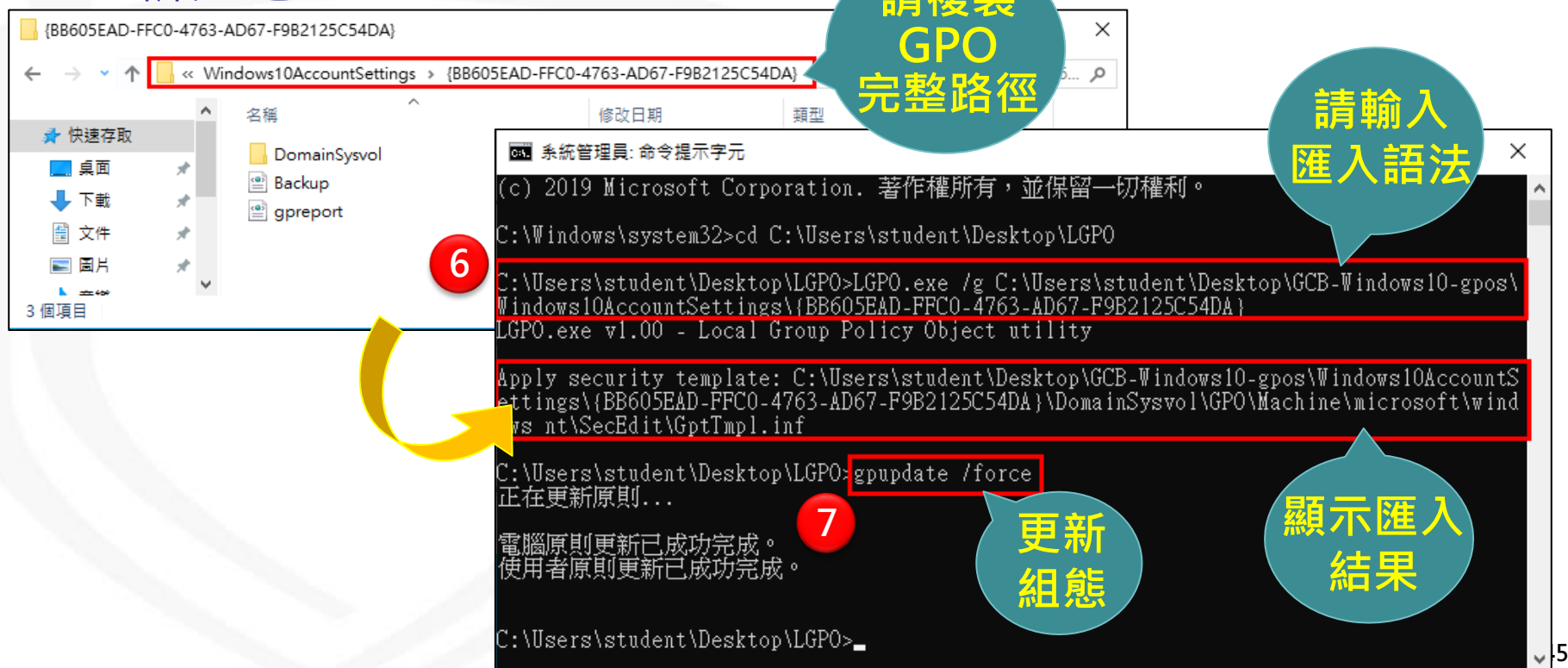
顯示備份  
結果



顯示備份  
結果

# 使用LGPO程式匯入GPO(3/3)

- 步驟6：於「命令提示字元」輸入指令  
**LGPO.exe /g <絕對路徑>**，將GPO檔案匯入電腦
- 步驟7：電腦重新開機或使用gpupdate /force指令更新組態



The screenshot illustrates the process of importing a GPO using the LGPO utility. It is divided into two main parts: a File Explorer window and a Command Prompt window.

**File Explorer (Left):** Shows the path `Windows10AccountSettings > {BB605EAD-FFC0-4763-AD67-F9B2125C54DA}` selected. A red box highlights this path, with a callout bubble saying "請複製 GPO 完整路徑" (Please copy the complete GPO path).

**Command Prompt (Right):** Shows the execution of the LGPO utility. A red circle with the number "6" points to the command line:  
`C:\Users\student\Desktop\LGPO>LGPO.exe /g C:\Users\student\Desktop\GCB-Windows10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}`  
A callout bubble says "請輸入 匯入語法" (Please enter import syntax). Below this, the output shows the security template being applied. A red circle with the number "7" points to the command:  
`C:\Users\student\Desktop\LGPO>gpupdate /force`  
A callout bubble says "更新組態" (Update configuration). The final output shows "電腦原則更新已成功完成。" (Computer policy update successful). A callout bubble says "顯示匯入結果" (Display import results).

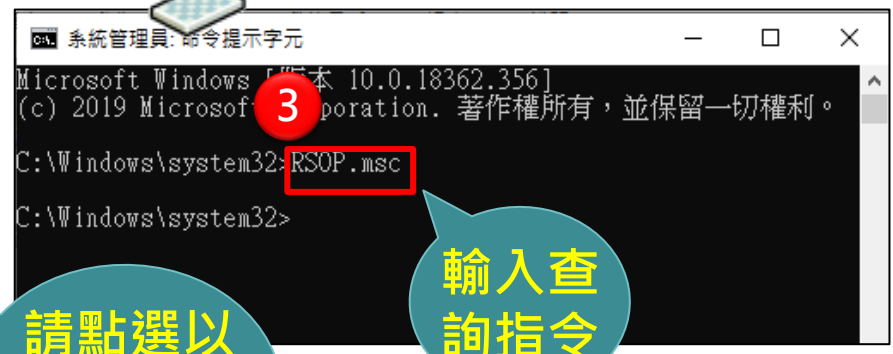
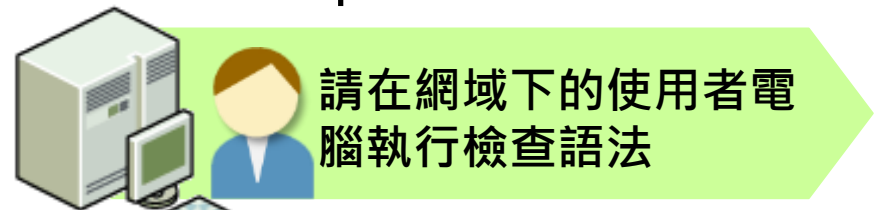
# GPO套用狀況檢查方式

NCCST

# AD環境下的檢查方式(1/4)

- 使用RSOP檢查群組原則

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
- 步驟2：點選「**以系統管理員身分執行**」
- 步驟3：於「命令提示字元」輸入rsop.msc查詢群組原則結果



# 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  
模式  
使用者名稱  
顯示使用者原則設定值  
電腦名稱  
顯示電腦原則設定值

設定  
記錄  
GCB\student  
是  
GCB  
是

顯示群組原則套用結果

原則結果組

檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)

原則	電腦設定	來源 GPO
使用可還原的加密來存放密碼	已停用	Windows10AccountSettings
密碼必須符合複雜性需求	已啟用	Windows10AccountSettings
密碼最長使用期限	90 天	Windows10AccountSettings
密碼最短使用期限	1 天	Windows10AccountSettings
強制執行密碼歷程記錄	3 記憶的密碼	Windows10AccountSettings
最小密碼長度	8 個字元	Windows10AccountSettings

student 在 DESKTOP-WIN10 - RSoP

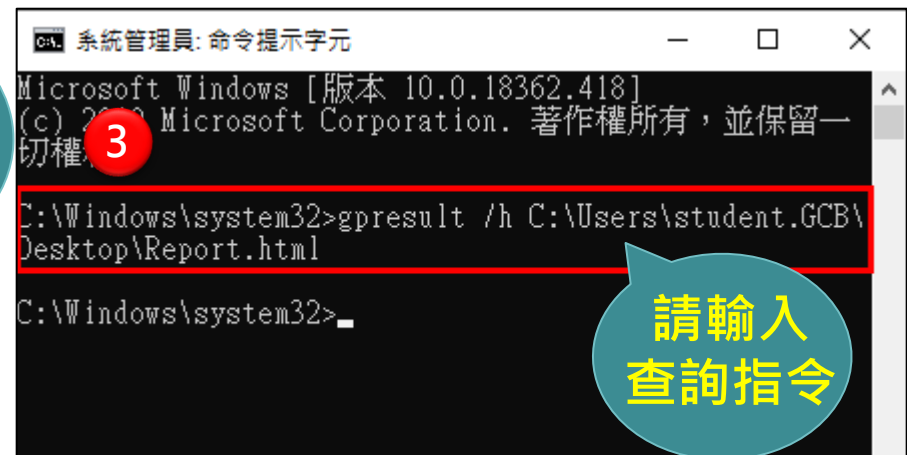
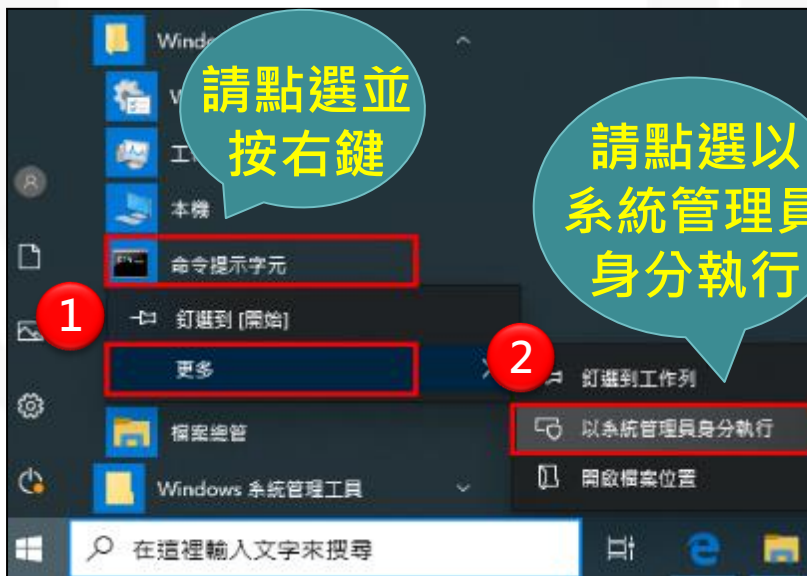
- 電腦設定
  - 軟體設定
  - Windows 設定
    - 安全性設定
      - 帳戶原則
        - 密碼原則
        - 帳戶鎖定原則
      - 本機原則
        - 稽核原則
        - 使用者權限指派
        - 安全性選項
      - 事件記錄檔
      - 受限群組
      - 系統服務
      - 登錄



# AD環境下的檢查方式(3/4)

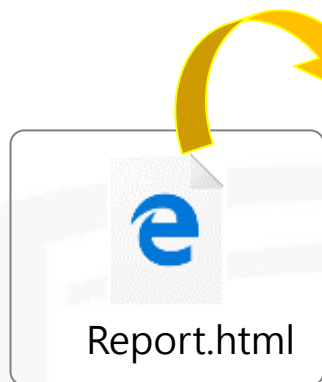
- 使用gpresult檢查群組原則

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
- 步驟2：點選「**以系統管理員身分執行**」
- 步驟3：於「命令提示字元」輸入gpresult /h <檔案儲存路徑>\檔名.html



# AD環境下的檢查方式(4/4)

- 使用gpresult檢查群組原則，顯示如下



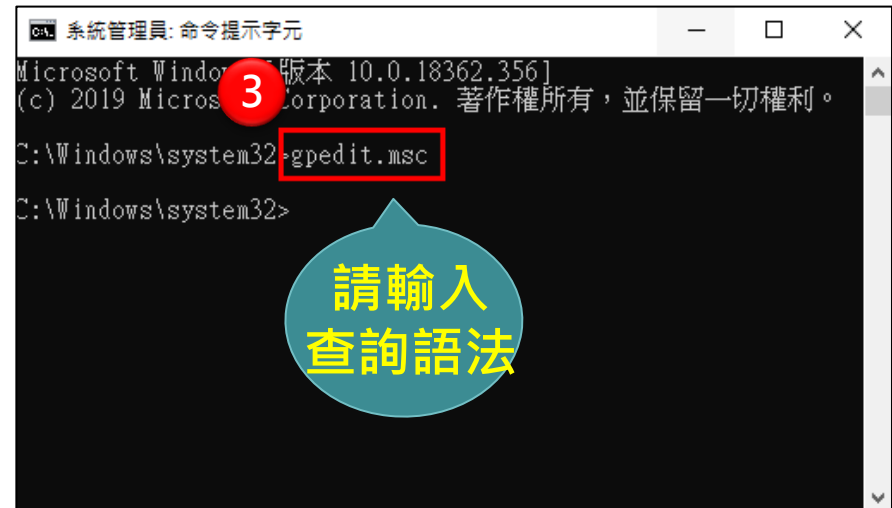
群組原則結果		
GCB\DESKTOP-WIN10 的 GCB\student		
資料收集: 2019/10/12 上午 01:54:05		全部隱藏
摘要		顯示
電腦詳細資料		隱藏
一般		顯示
元件狀態		顯示
設定		隱藏
原則		隱藏
Windows 設定		隱藏
安全性設定		隱藏
帳戶原則/密碼規則		隱藏
原則	設定	優勢 GPO
使用可遺原的加密來存放密碼	已停用	Windows10AccountSettings
密碼必須符合複雜性需求	已啟用	Windows10AccountSettings
密碼長度最小值	8 個字元	Windows10AccountSettings
密碼最長使用期限	90 天	Windows10AccountSettings
密碼最短使用期限	1 天	Windows10AccountSettings
強制密碼歷程記錄	已記憶 3 個密碼	Windows10AccountSettings
帳戶原則/帳戶鎖定原則		隱藏
原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分鐘	Windows10AccountSettings
帳戶鎖定期間	15 分鐘	Windows10AccountSettings

顯示群組  
原則套用  
結果

# 單機環境下的檢查方式(1/2)

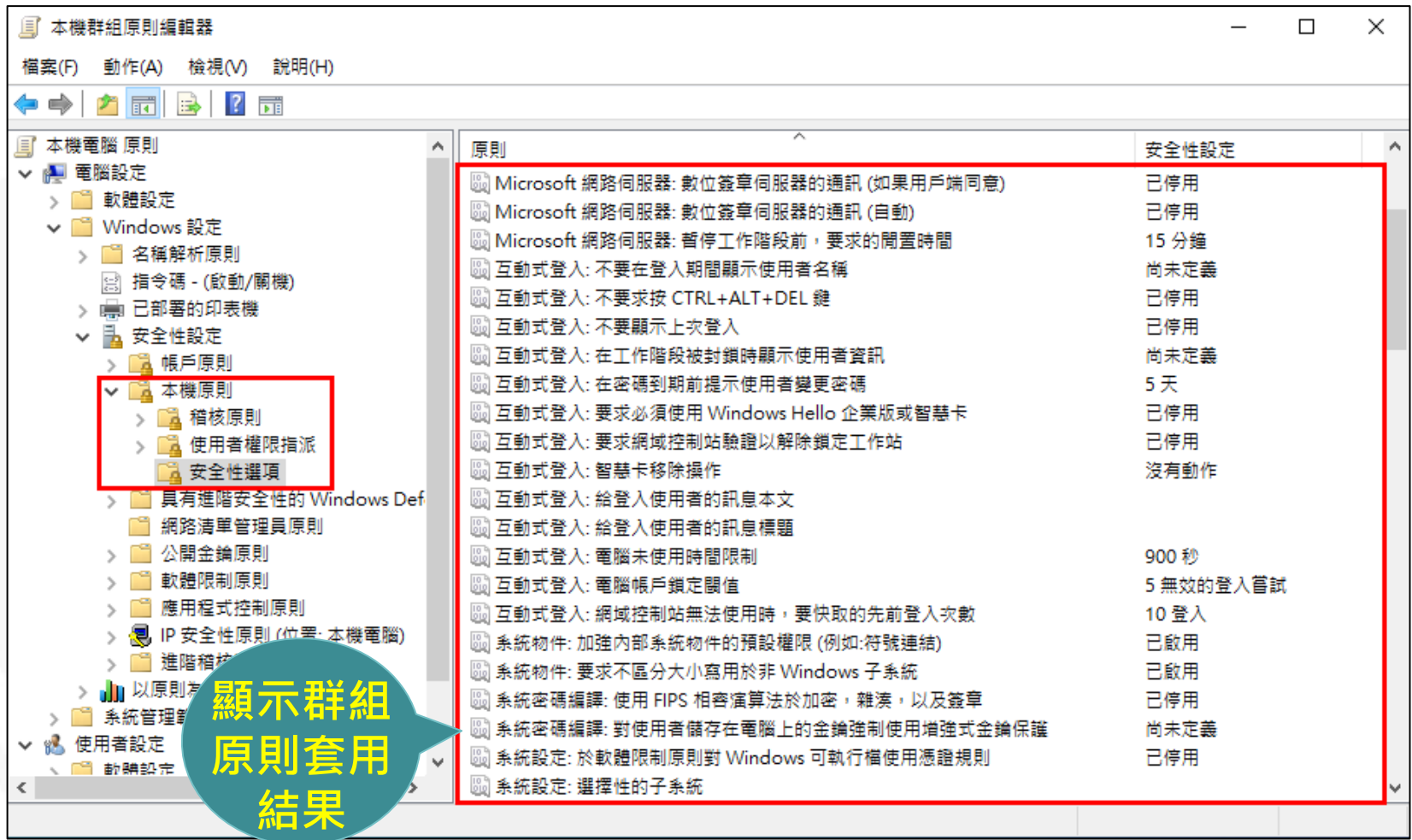
- 使用gpedit.msc檢查群組原則

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
- 步驟2：點選「**以系統管理員身分執行**」
- 步驟3：於「命令提示字元」輸入gpedit.msc查詢本機群組原則結果



# 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



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
    - 名稱解析原則
    - 指令碼 - (啟動/關機)
    - 已部署的印表機
    - 安全性設定
      - 帳戶原則
      - 本機原則**
        - 稽核原則
        - 使用者權限指派
        - 安全性選項
      - 具有進階安全性的 Windows Def
      - 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
    - 以原則為基礎的
    - 系統管理
  - 使用者設定
    - 軟體設定

原則	安全性設定
Microsoft 網路伺服器: 數位簽章伺服器的通訊 (如果用戶端同意)	已停用
Microsoft 網路伺服器: 數位簽章伺服器的通訊 (自動)	已停用
Microsoft 網路伺服器: 暫停工作階段前, 要求的閒置時間	15 分鐘
互動式登入: 不要在登入期間顯示使用者名稱	尚未定義
互動式登入: 不要求按 CTRL+ALT+DEL 鍵	已停用
互動式登入: 不要顯示上次登入	已停用
互動式登入: 在工作階段被封鎖時顯示使用者資訊	尚未定義
互動式登入: 在密碼到期前提示使用者變更密碼	5 天
互動式登入: 要求必須使用 Windows Hello 企業版或智慧卡	已停用
互動式登入: 要求網域控制站驗證以解除鎖定工作站	已停用
互動式登入: 智慧卡移除操作	沒有動作
互動式登入: 給登入使用者的訊息本文	
互動式登入: 給登入使用者的訊息標題	
互動式登入: 電腦未使用時間限制	900 秒
互動式登入: 電腦帳戶鎖定閾值	5 無效的登入嘗試
互動式登入: 網域控制站無法使用時, 要快取的先前登入次數	10 登入
系統物件: 加強內部系統物件的預設權限 (例如: 符號連結)	已啟用
系統物件: 要求不區分大小寫用於非 Windows 子系統	已啟用
系統密碼編譯: 使用 FIPS 相容演算法於加密, 雜湊, 以及簽章	已停用
系統密碼編譯: 對使用者儲存在電腦上的金鑰強制使用增強式金鑰保護	尚未定義
系統設定: 於軟體限制原則對 Windows 可執行檔使用憑證規則	已停用
系統設定: 選擇性的子系統	

顯示群組原則套用結果

# 恢復原始設定之方式

NCCST

# AD環境下恢復原始設定方式

- 步驟1：點選欲取消GPO連結之組織單位(OU)
- 步驟2：在已連結的群組原則物件頁面，選取欲取消連結的GPO按滑鼠**右鍵**
- 步驟3：點選「刪除」將GPO自組織單位中移除
- 步驟4：當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



The screenshot illustrates the process of removing a Group Policy Object (GPO) link from an Active Directory (AD) environment. It is divided into four numbered steps:

- Step 1:** In the Group Policy Management console, the 'Technical Services Center' (技術服務中心) is selected under the 'gcb.gov.tw' domain.
- Step 2:** The 'Linked Group Policy Objects' (已連結的群組原則物件) tab is active, showing a table with columns for 'Link Order' (連結順序), 'GPO', and 'Enforced' (強制). The 'Windows10AccountSettings' GPO is selected.
- Step 3:** A right-click context menu is open over the selected GPO, and the 'Delete' (刪除) option is highlighted.
- Step 4:** A Command Prompt window shows the execution of the command `gpupdate /force`, which successfully updates the group policy.

A callout bubble with the text "請點選並按右鍵" (Please click and right-click) points to the selected GPO in the table.

# 單機環境下恢復原始設定方式(1/4)



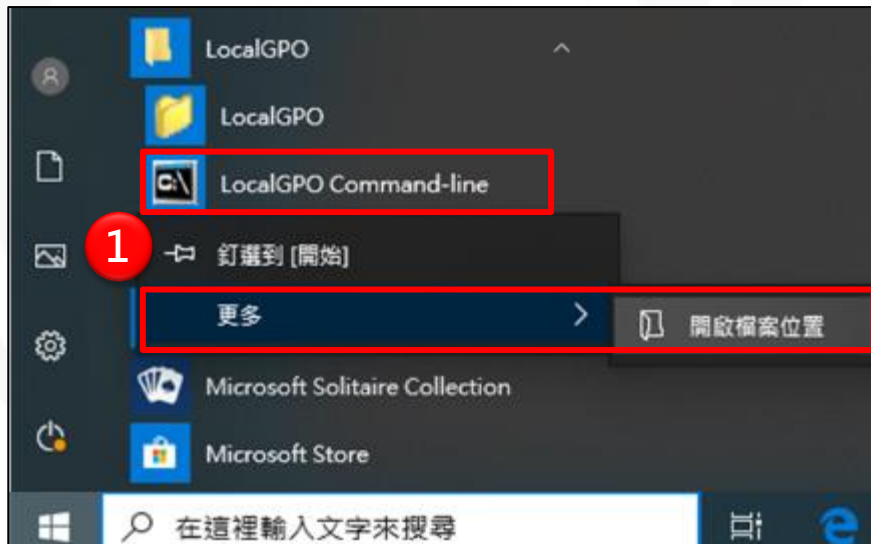
## ● 使用LocalGPO恢復原始設定

– 步驟1：點擊開始→LocalGPO資料夾→點選

「LocalGPO Command-line」按滑鼠**右鍵**→更多→開啟檔案位置

– 步驟2：點選「LocalGPO Command-line」按滑鼠**右鍵**

– 步驟3：選擇「以系統管理員身分執行」



# 單機環境下恢復原始設定方式(2/4)



- 使用LocalGPO恢復原始設定

- 步驟4：於「LocalGPO Command-line」輸入  
cscript LocalGPO.wsf /Restore

- 步驟5：電腦重新開機或使用gpupdate/force指令更新組態

```
系統管理員: LocalGPO Command-line
C:\Program Files (x86)\LocalGPO>cscript LocalGPO.wsf /Restore
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corp. 1996-2006, 著作權所有, 並保留一切權利。

Modifying Local Policy... this process can take a few moments.
Restoring Security Settings...
Restoring Administrative Template settings...
Restoring Advanced Audit Policy...
Restoring MLGPO...
Refreshing Local Group Policy...

Local Policy default values restored!

Please restart the computer to refresh the Local Policy

C:\Program Files (x86)\LocalGPO>gpupdate /force
正在更新原則...
```

請輸入  
恢復原始  
設定語法

顯示復原  
結果

更新  
組態

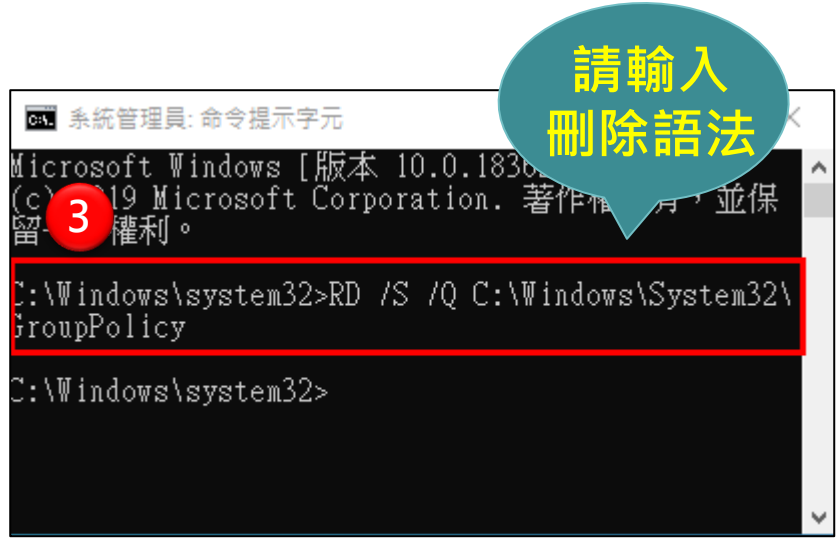
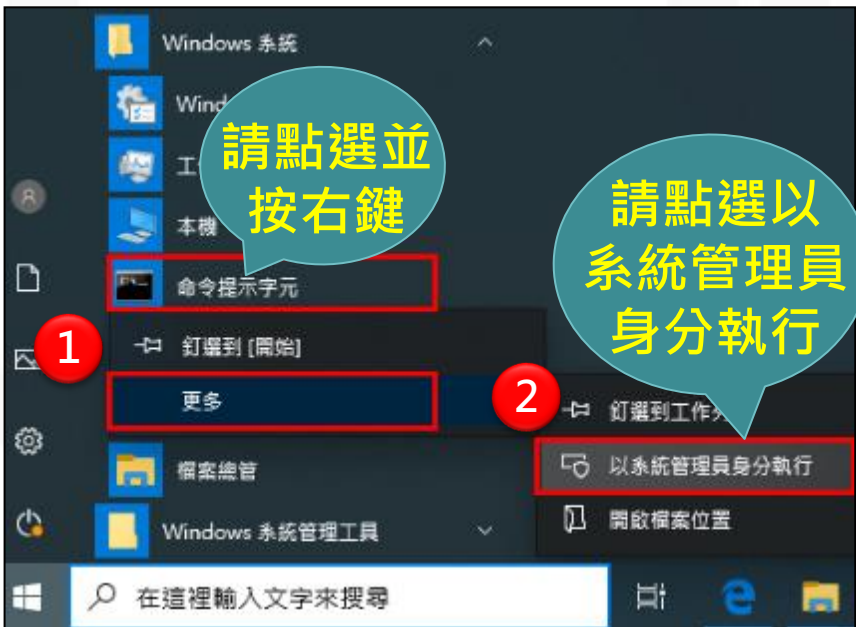


# 單機環境下恢復原始設定方式(3/4)



- 使用LGPO恢復原始設定

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
- 步驟2：選擇「**以系統管理員身分執行**」
- 步驟3：於「命令提示字元」輸入刪除群組原則指令  
RD /S /Q C:\Windows\System32\GroupPolicy



# 單機環境下恢復原始設定方式(4/4)



## ● 使用LGPO恢復原始設定

- 步驟4：於「命令提示字元」輸入cd <LGPO應用程式完整目錄路徑>，切換至LGPO目錄
- 步驟5：於「命令提示字元」輸入LGPO.exe /g <組態備份檔的絕對路徑> **匯入備份的GPO檔案**
- 步驟6：重新開機或使用gpupdate /force指令更新組態

請輸入切  
換目錄語法

```
系統管理員: 命令提示字元
C:\Windows\system32>cd C:\Users\student\Desktop\LGPO
C:\Users\student\Desktop\LGPO>LGPO.exe /g C:\Users\student\Desktop\BackupFile\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}
LGPO.exe v1.00 - Local Group Policy Object utility

Audit policy directory exists
Copied C:\Users\student\Desktop\BackupFile\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}\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\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\Users\student\Desktop\BackupFile\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}\DomainSysvol\GPO\Machine\registry.pol
Import Machine settings from registry.pol: C:\Users\student\Desktop\BackupFile\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}\DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\Users\student\Desktop\BackupFile\{9E9D2CE4-C0A4-4711-94AA-AA8062D44417}\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>
```

請輸入  
匯入語法

更新組態  
設定

# 例外管理調整GCB設定値

NCCST

# 例外管理說明

- 套用GCB後，若發生系統異常或無法使用，導致影響日常公務，則可視需求調整設定值並進行例外管理

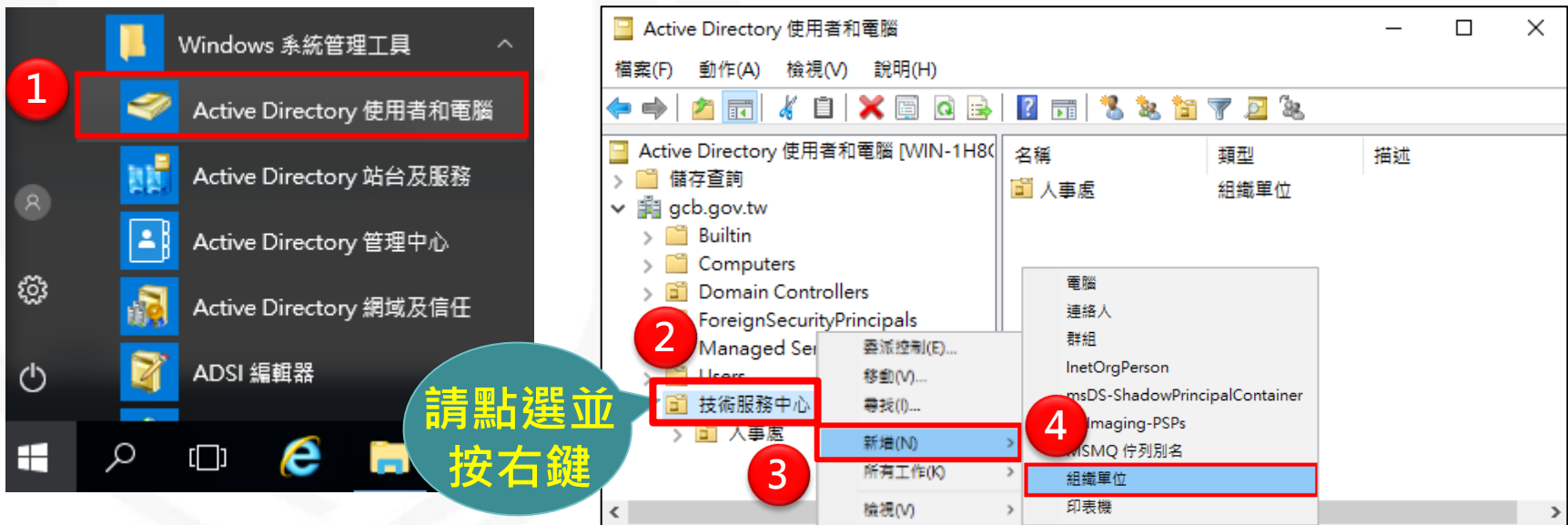


# AD環境下調整與測試GCB

NCCST

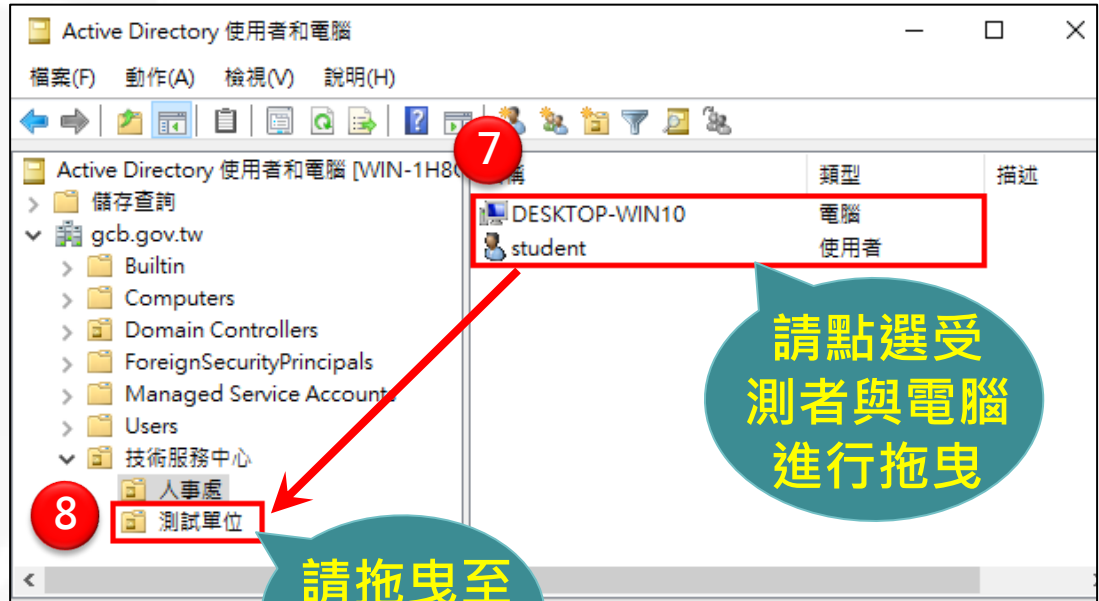
# 建立測試組織單位(OU)(1/2)

- 步驟1：點擊開始→Windows系統管理工具→點擊Active Directory使用者和電腦
- 步驟2：在「技術服務中心」組織單位按滑鼠右鍵
- 步驟3：點選「新增」
- 步驟4：點選「組織單位」



# 建立測試組織單位(OU)(2/2)

- 步驟5：在「名稱」欄位輸入測試的組織單位名稱
- 步驟6：點選「確定」按鈕，完成建立測試組織單位
- 步驟7：點選受測之使用者與電腦
- 步驟8：拖曳至測試組織單位



# 建立測試的群組原則物件(1/2)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理
- 步驟3：在群組原則物件節點按滑鼠右鍵
- 步驟4：點選「新增」
- 步驟5：在「名稱」欄位輸入測試的群組原則物件名稱
- 步驟6：點選「確定」按鈕



請點選並按右鍵

名稱	GPO 狀態	WMI 篩選器	修改日期
Default Domain Con...	停用所有設定	無	2019/10
Default Domain Poli...	停用所有設定	無	2019/10

新增 GPO

名稱(N): Test\_Windows10AccountSettings

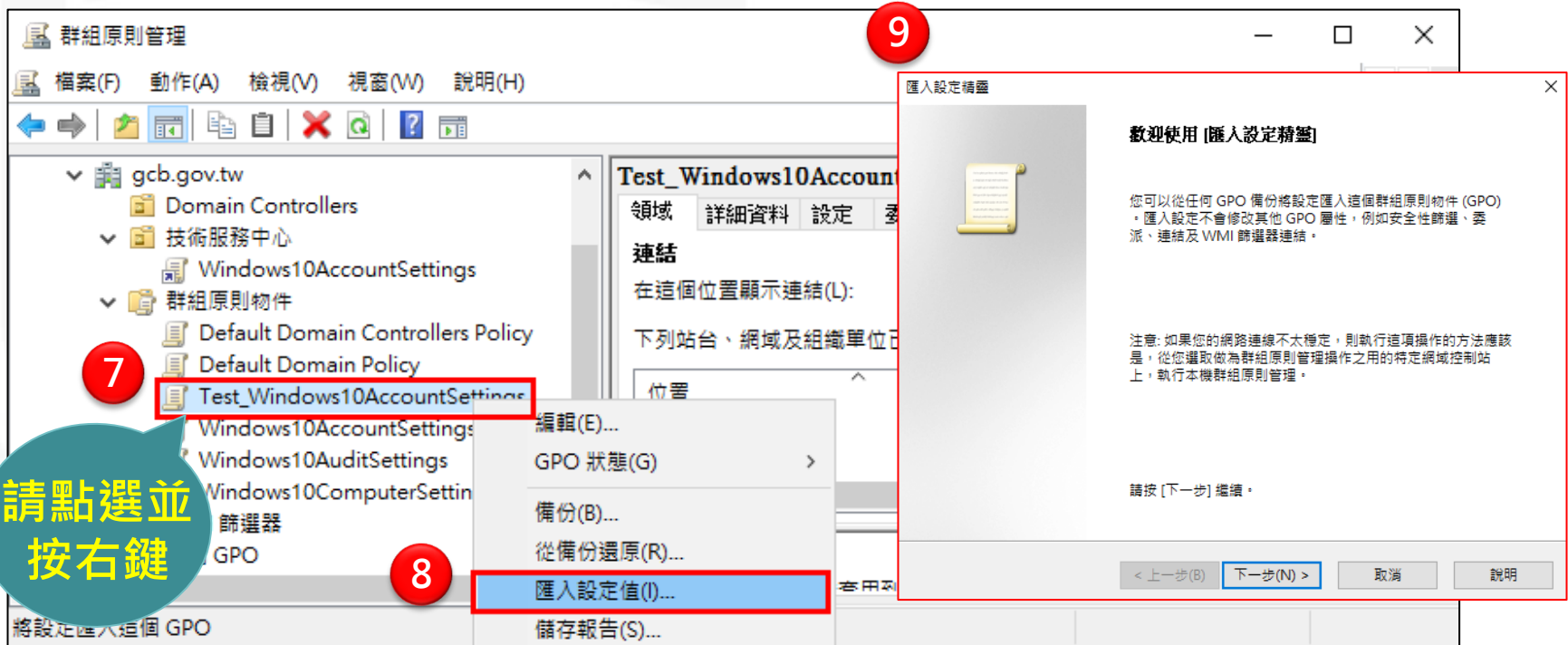
來源入門 GPO(S): (無)

確定 取消



# 建立測試的群組原則物件(2/2)

- 步驟7：點選測試的群組原則物件按滑鼠**右鍵**
- 步驟8：選擇「匯入設定值」
- 步驟9：透過【匯入設定精靈】功能，完成GPO設定檔匯入



群組原則管理

檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)

gcb.gov.tw

- Domain Controllers
- 技術服務中心
  - Windows10AccountSettings
  - 群組原則物件
    - Default Domain Controllers Policy
    - Default Domain Policy
    - Test\_Windows10AccountSettings**
    - Windows10AccountSettings
    - Windows10AuditSettings
    - Windows10ComputerSettings
    - 篩選器
    - GPO

Test\_Windows10AccountSettings

領域 詳細資料 設定 委派

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

7

請點選並按右鍵

8

9

匯入設定精靈

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，例如安全性篩選、委派、連結及 WMI 篩選器連結。

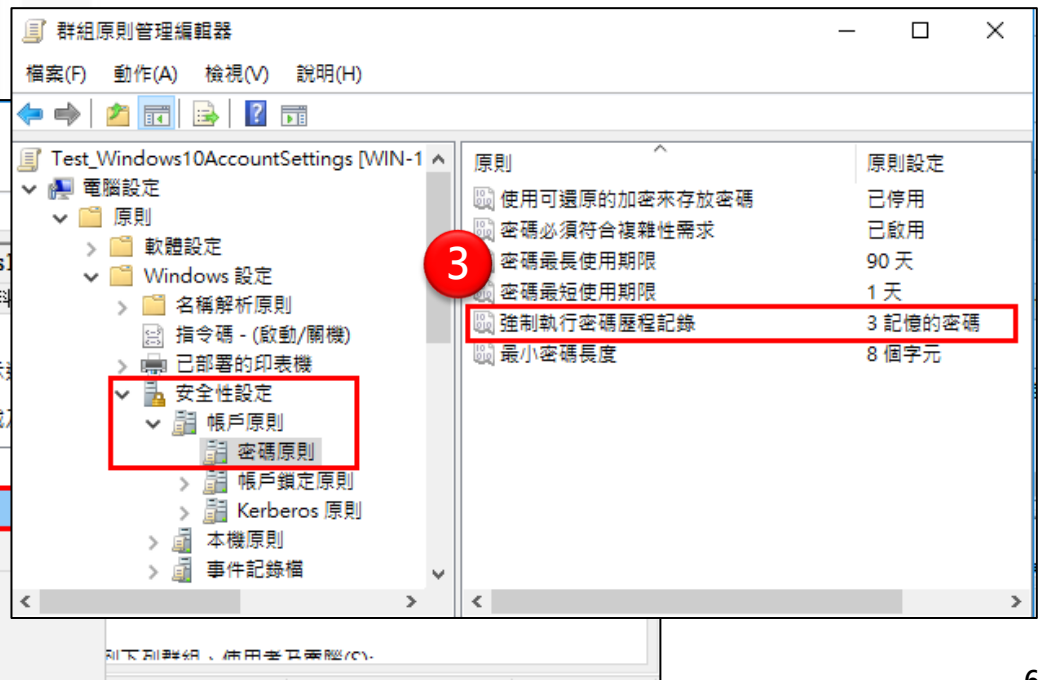
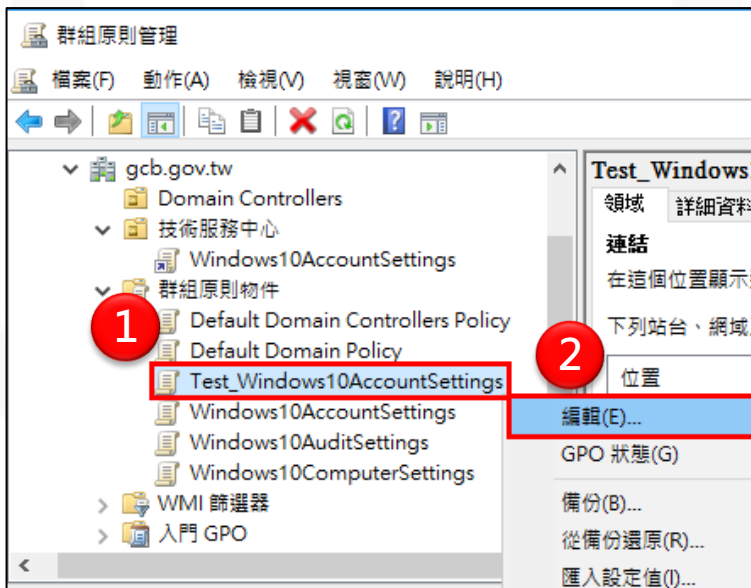
注意: 如果您的網路連線不太穩定，則執行這項操作的方法應該是，從您選取做為群組原則管理操作之用的特定網域控制站上，執行本機群組原則管理。

請按 [下一步] 繼續。

< 上一步(B) 下一步(N) > 取消 說明

# 調整測試項目設定值(1/2)

- 步驟1：在測試的GPO按滑鼠**右鍵**
- 步驟2：點選「編輯」，開啟「群組原則管理編輯器」
- 步驟3：點選2下欲調整之項目，以「強制執行密碼歷程記錄」為例(電腦設定\Windows\安全性設定\密碼原則)



# 調整測試項目設定值(2/2)

- 步驟4：調整「強制執行密碼歷程記錄」設定值
- 步驟5：點選「套用」按鈕
- 步驟6：點選「確定」按鈕



# 將測試GPO連結至測試組織單位



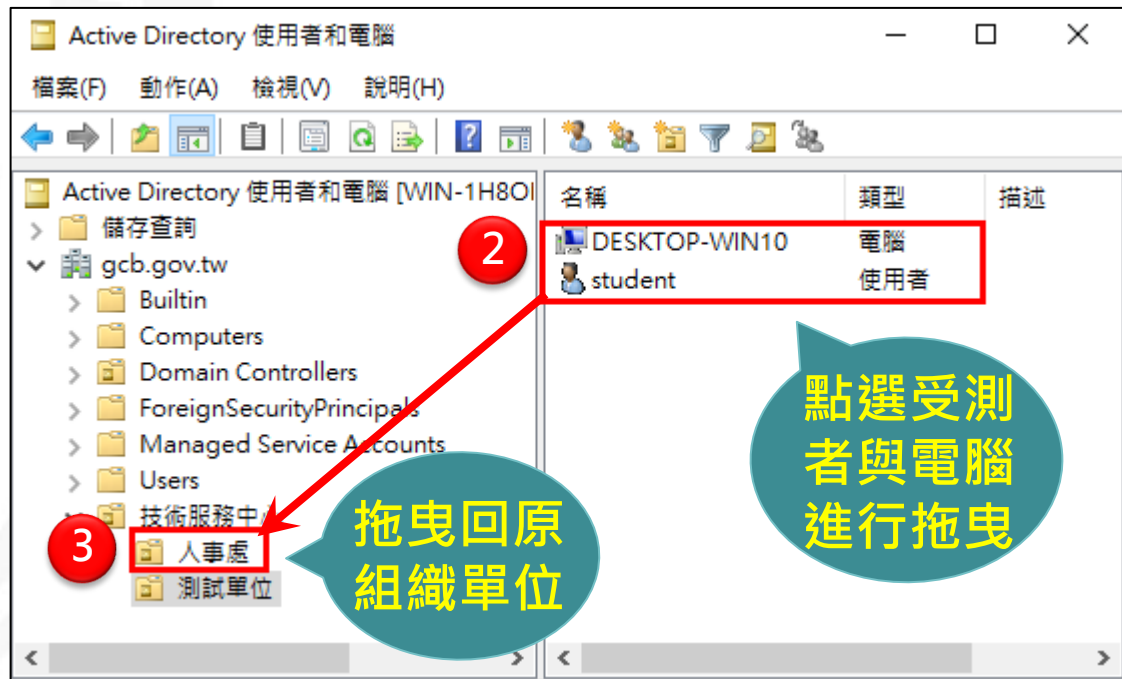
- 步驟1：點選調整後的測試GPO
- 步驟2：拖曳至「測試單位」
- 步驟3：點選「確定」按鈕，完成測試GPO連結至測試組織單位
- 步驟4：在使用者電腦上輸入gpupdate /force更新群組原則，測試新設定值並確認障礙已排除

The screenshot illustrates the process of linking a Group Policy Object (GPO) to a test Organizational Unit (OU) and updating it. It consists of several overlapping windows and callouts:

- Group Policy Management Console:** Shows the hierarchy of Group Policy Objects (GPOs) under the domain `gcb.gov.tw`. The GPO `Test_Windows10AccountSettings` is selected and highlighted with a red box and a callout bubble (1) that says "請點選 GPO 進行拖曳" (Please click the GPO for dragging).
- Group Policy Objects List:** Shows the list of GPOs, with `Test_Windows10AccountSettings` highlighted and a callout bubble (2) that says "請拖曳 GPO 到 組織單位" (Please drag the GPO to the organizational unit).
- Test Organizational Unit (OU):** The OU `Test_Units` is selected in the left pane, and a callout bubble (3) points to it.
- Confirmation Dialog:** A dialog box asks "您要將選取的 GPO 連結到這個組織單位嗎?" (Do you want to link the selected GPO to this organizational unit?). The "確定" (OK) button is highlighted with a red box and a callout bubble (4) that says "輸入更新群組原則語法" (Enter update group policy syntax).
- Command Prompt:** A command prompt window shows the command `gpupdate /force` being entered and executed. A callout bubble (5) points to the command, saying "輸入更新群組原則語法" (Enter update group policy syntax).

# 受測電腦與使用者放回原單位

- 步驟1：點擊開始→Windows系統管理工具→點擊Active Directory使用者和電腦
- 步驟2：點選受測之使用者與電腦
- 步驟3：拖曳回其所屬之組織單位



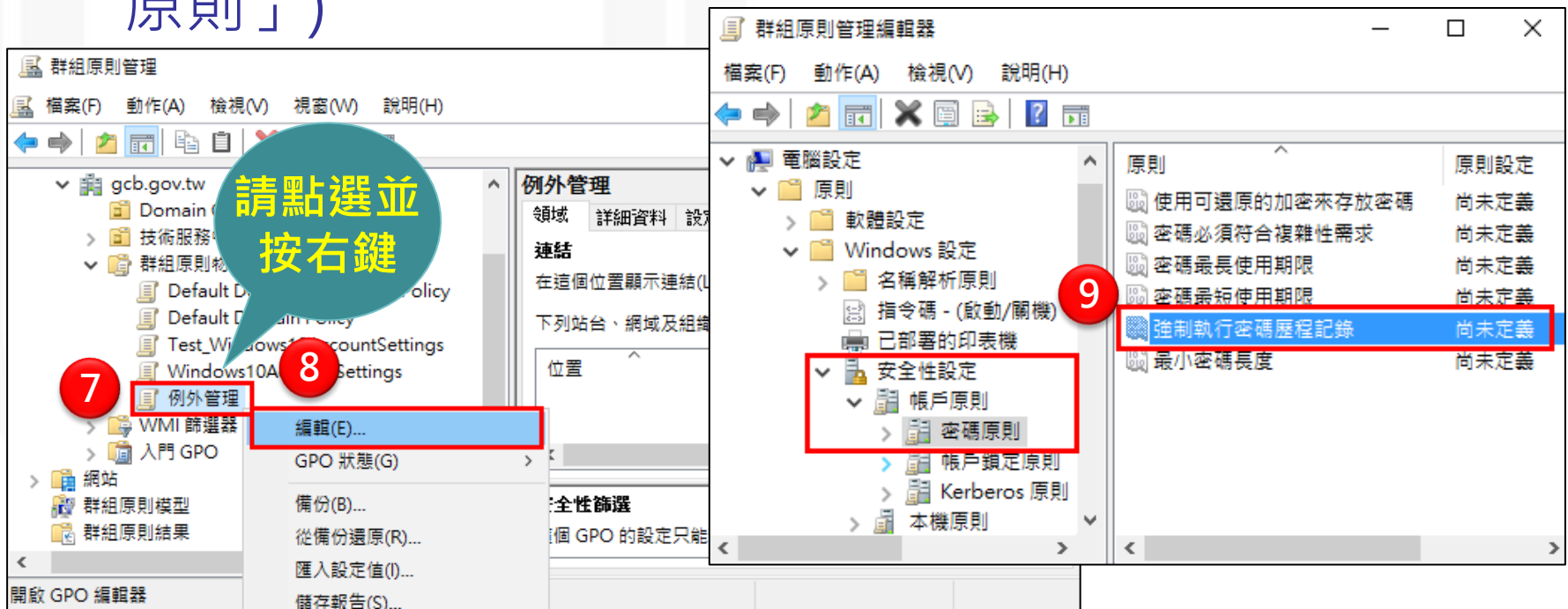
# 建立例外管理GPO(1/3)

- 步驟1：點擊開始→所有程式→系統管理工具
- 步驟2：點擊群組原則管理
- 步驟3：在群組原則物件節點按滑鼠**右鍵**
- 步驟4：點選「新增」
- 步驟5：在「名稱」欄位輸入例外管理的群組原則物件名稱
- 步驟6：點選「確定」按鈕



# 建立例外管理GPO(2/3)

- 步驟7：在例外管理GPO按滑鼠右鍵
- 步驟8：點選「編輯」，開啟「群組原則管理編輯器」
- 步驟9：點選欲開設例外項目，以「強制執行密碼歷程記錄」為例(電腦設定\Windows\安全性設定\密碼原則)」



# 建立例外管理GPO(3/3)

- 步驟10：調整「強制執行密碼歷程記錄」設定值
- 步驟11：點選「套用」按鈕
- 步驟12：點選「確定」按鈕





# 將例外管理GPO連結至組織單位(OU)

- 步驟1：點選例外管理GPO
- 步驟2：拖曳至「人事處」組織單位
- 步驟3：點選「確定」按鈕，完成連結
- 步驟4：點選「人事處」組織單位
- 步驟5：將例外管理GPO順序調整至第一順位



請點選 GPO 拖曳

請拖曳 GPO 到 組織單位

使用按鍵 調整順序

連結順序	GPO	強制
1	例外管理	否
2	Windows10AccountSettings	否

3

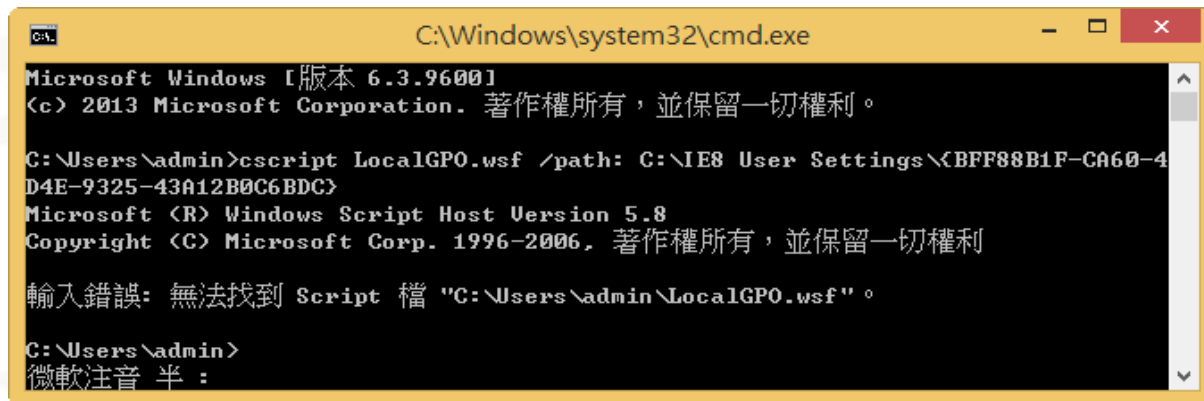
# 常見問答

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.

NCCST

## Q1

LocalGPO匯入失敗(Path not found)之解決方式?



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\admin>cscript LocalGPO.wsf /path: C:\IE8 User Settings\{BFF88B1F-CA60-4D4E-9325-43A12B0C6BDC}
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corp. 1996-2006. 著作權所有，並保留一切權利

輸入錯誤: 無法找到 Script 檔 "C:\Users\admin\LocalGPO.wsf"。

C:\Users\admin>
微軟注音 半 :
```

– 移除目錄名稱中的空白

➤ 如將「IE8 User Settings」調整為「IE8UserSettings」

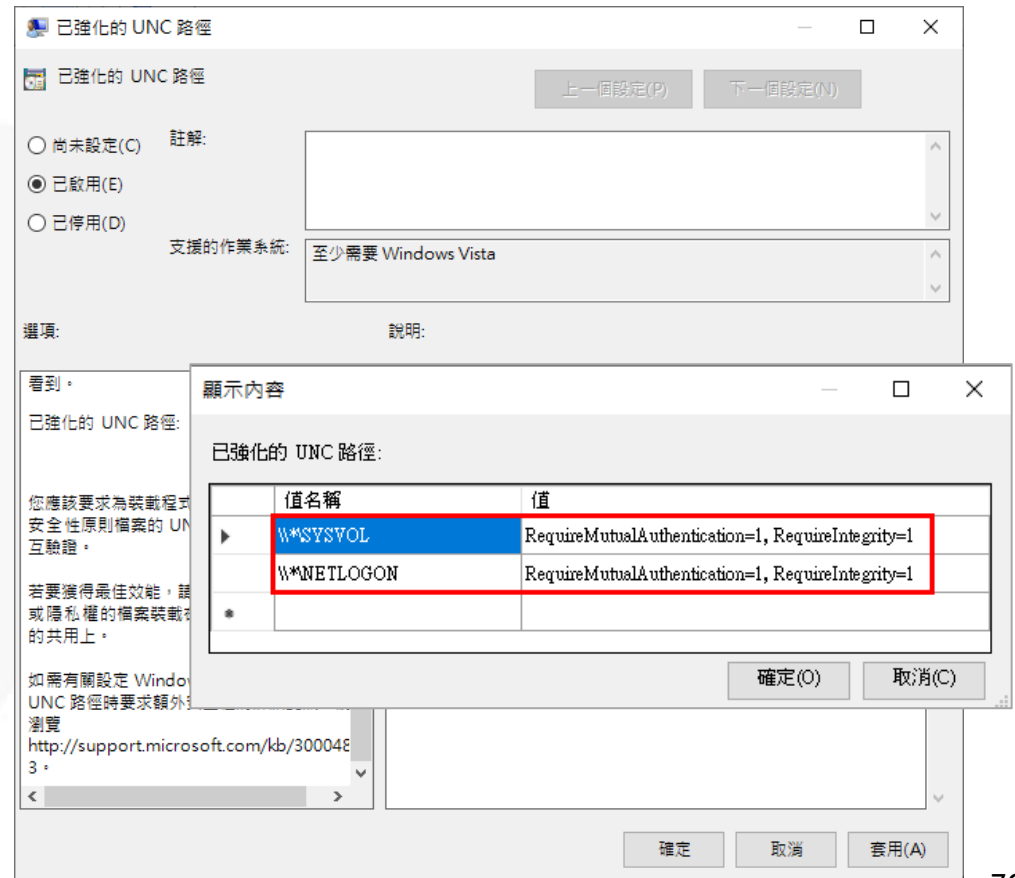
– 匯入時將資料夾名稱前後加入雙引號

➤ cscript LocalGPO.wsf /path: "C:\IE8 User Settings\{BFF88B1F-CA60-4D4E-9325-43A12B0C6BDC}"

# 常見問答(2/12)

**Q2** 若UNC路徑未設定在「已強化的UNC路徑」清單中，是否會受此項組態設定影響？

—此項組態設定只會影響設定於「\\\*\SYSVOL」與「\\\*\NETLOGON」清單中之UNC路徑，其餘路徑不受影響



已強化的 UNC 路徑

上一個設定(P) 下一個設定(N)

尚未設定(C) 註解: [ ]

已啟用(E)

已停用(D)

支援的作業系統: 至少需要 Windows Vista

選項: [ ] 說明: [ ]

看到: [ ]

已強化的 UNC 路徑:

您應該要求為裝載程式安全性原則檔案的 UNC 互驗證。

若要獲得最佳效能，請或隱私權的檔案裝載的共用上。

如需有關設定 Windows UNC 路徑時要求額外瀏覽

<http://support.microsoft.com/kb/3000483>

值名稱	值
\\*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1
\\*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1

確定(O) 取消(C)

確定 取消 套用(A)

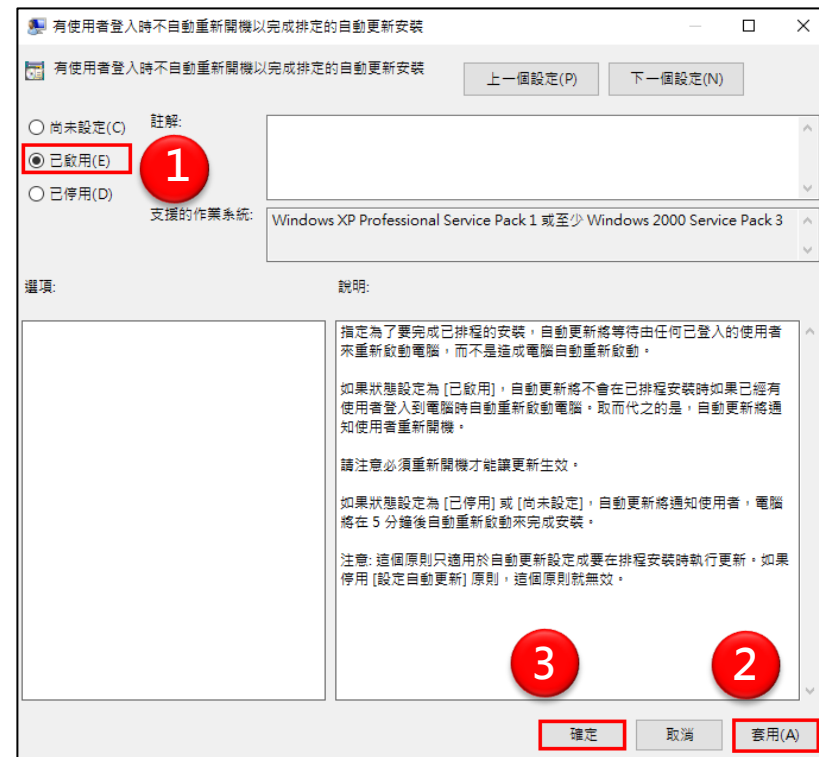
# 常見問答(3/12)

## Q3 如何解決Windows Update自動更新造成使用者於登入時自動重新開機之狀況？

—如因公務執行需求，可調整

### CCE-42867-2設定值

- 步驟1：點選「有使用者登入時不自動重新開機以完成排定的自動更新安裝」(電腦設定\系統管理範本\Windows元件\Windows Update)，將設定值調整為「啟用」
- 步驟2：點選「套用」按鈕
- 步驟3：點選「確定」按鈕



# 常見問答(4/12)

**Q4** 如何解決Windows市集App(如：相片、計算機)無法使用的問題？

**Q5** 如何解決Miracast投影功能無法使用的問題？

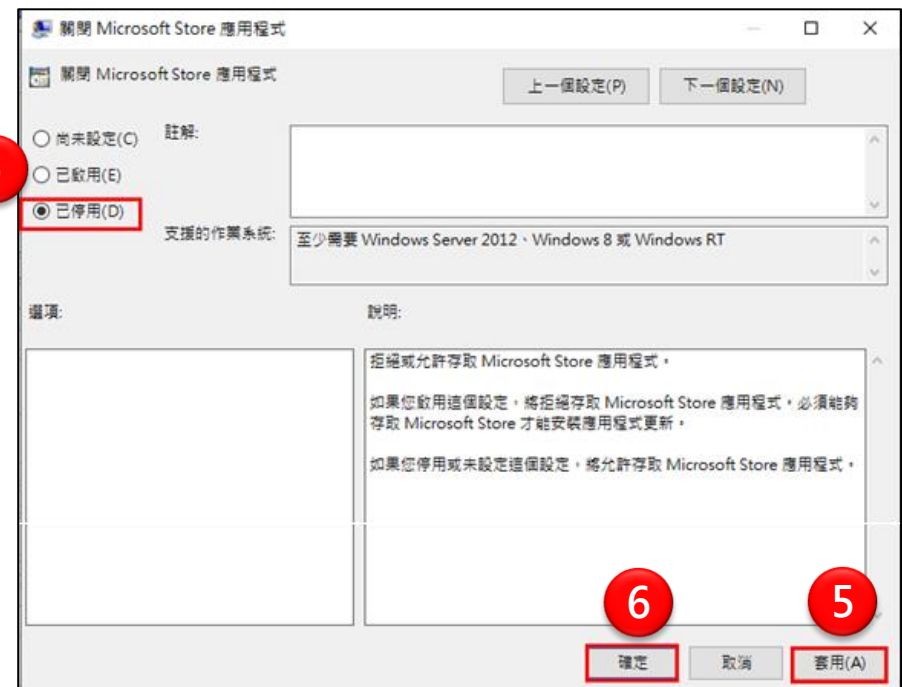
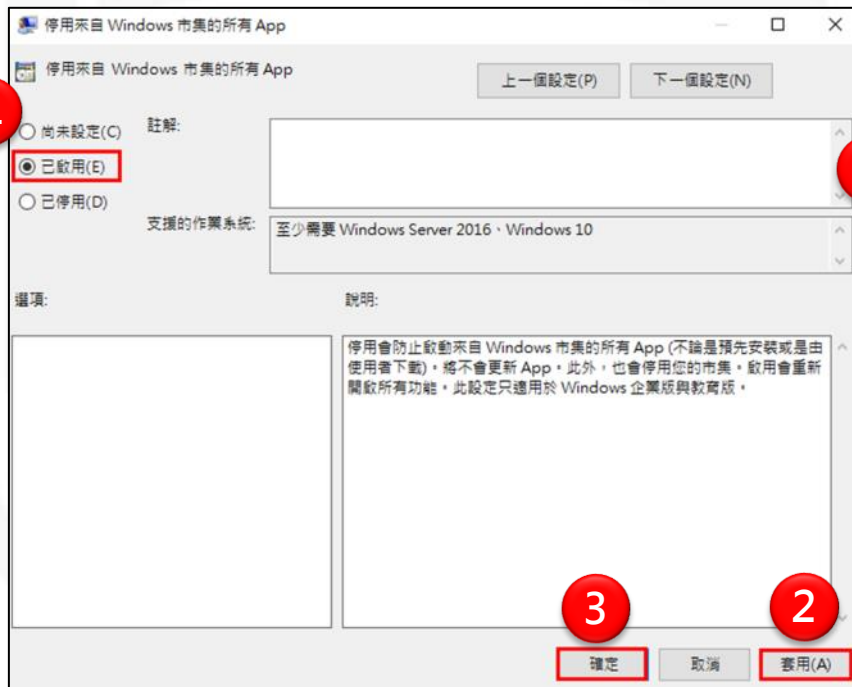
–因公務執行需求，可調整CCE-43814-3與CCE-42144-6設定值

- 步驟1：點選「停用來自Microsoft Store 的所有應用程式」(電腦設定\系統管理範本\Windows元件\市集)，將設定值調整為「啟用」
- 步驟2：點選「套用」按鈕
- 步驟3：點選「確定」按鈕

# 常見問答(5/12)



- 步驟4：點選「關閉Microsoft Store 應用程式」(電腦設定\系統管理範本\Windows元件\市集)，將設定值調整為「停用」
- 步驟5：點選「套用」按鈕
- 步驟6：點選「確定」按鈕



# 常見問答(6/12)

Q6

是否需以Windows Server 2016網域主機部署Windows 10電腦政府組態基準 ( GCB ) 呢？

- 建議使用Windows Server 2016網域主機部署Windows 10電腦政府組態基準(GCB)，若使用非Server 2016網域主機，仍可完整套用GCB，但無法檢視或修改部分組態設定值，需額外再安裝Windows 10管理範本或改用Security Compliance Manager(SCM)進行編輯

Q7

「設定6to4狀態」啟用後，該如何設定子選項？

- Windows 10政府組態基準(GCB)規範以公告之說明文件為基準，若建議設定值未指定子選項，則代表GCB針對子選項無規範設定值，機關可自行訂立此項標準



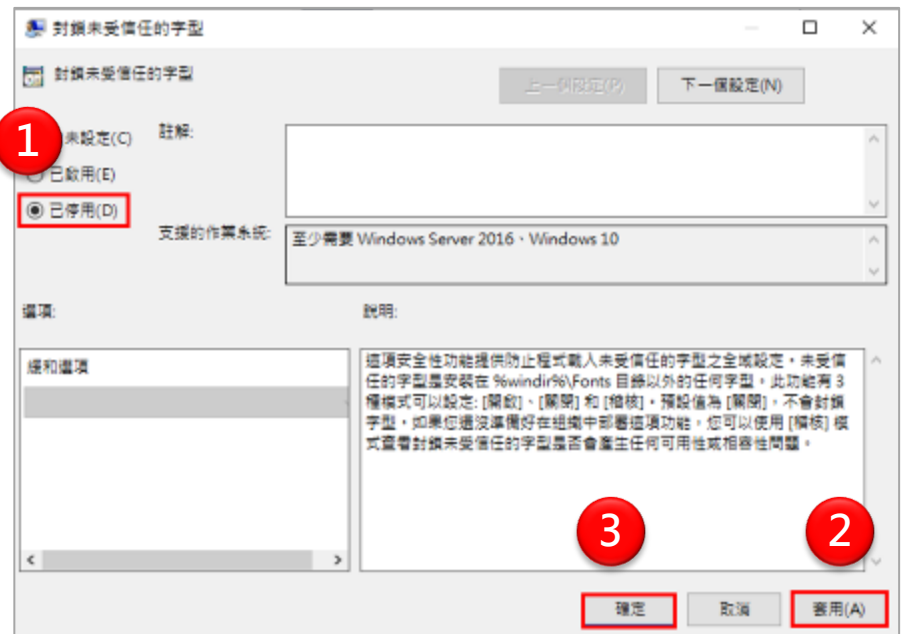
# 常見問答(7/12)



套用政府組態基準(GCB)後，造成公文系統圖示(icon)無法顯示，該怎麼辦？

–若公文系統以特殊字型做為圖示，必須調整CCE-43801-0設定值

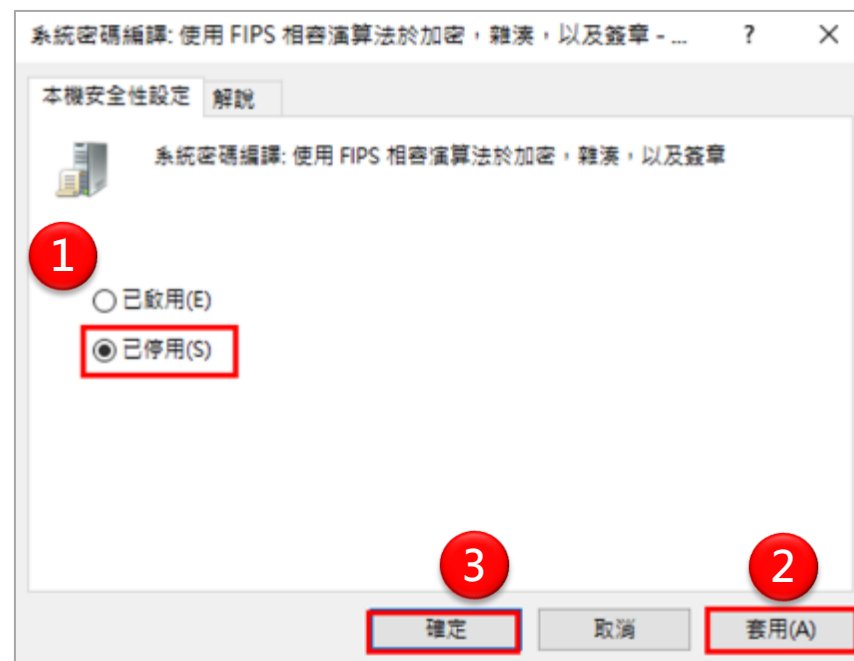
- 步驟1：點選「封鎖未受信任的字型」(電腦設定\系統管理範本\系統\緩和選項)，將設定值調整為「停用」
- 步驟2：點選「套用」按鈕
- 步驟3：點選「確定」按鈕



## Q9 如何解決Bitlocker加密磁碟機無法寫入問題？

– 如因公務執行需求，可調整CCE-42459-8設定值

- 步驟1：點選「系統加密編譯：使用FIPS 140相容加密演算法，包括加密、雜湊以及簽署演算法」(路徑為電腦設定\Windows元件\安全性設定\本機原則\安全性選項)，將設定值調整為「停用」
- 步驟2：點選「套用」按鈕
- 步驟3：點選「確定」按鈕



# 常見問答(9/12)

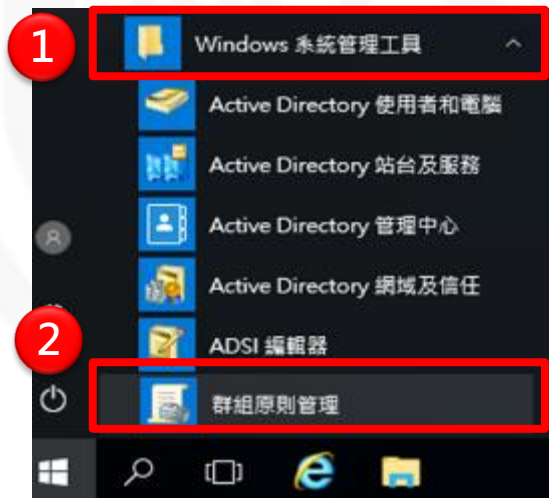


## Q10

機關內電腦劃分IE 8 與IE 11瀏覽器，如何讓AD可自動判斷瀏覽器版本，進而套用專版GPO？

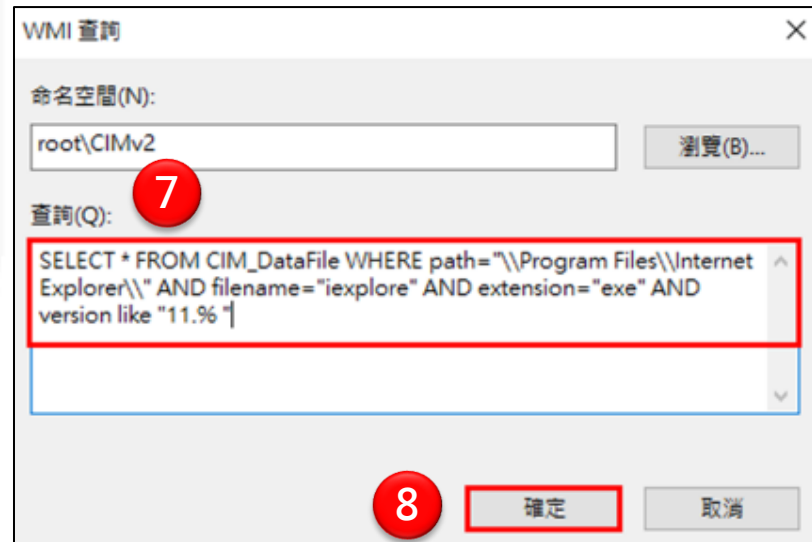
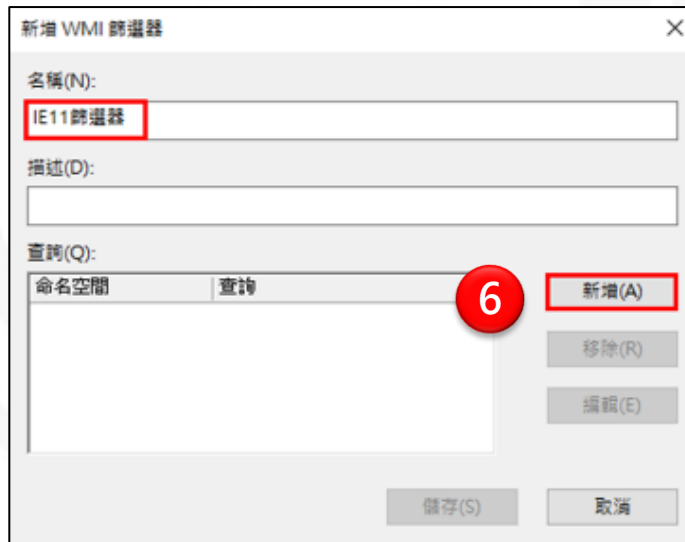
– 透過WMI篩選判斷各版本瀏覽器應套用之GPO版本

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理
- 步驟3：在WMI篩選器節點按滑鼠右鍵
- 步驟4：點選「新增」



# 常見問答(10/12)

- 步驟5：在新增WMI篩選器視窗，「名稱」欄位輸入WMI篩選器名稱，此以建立「IE11篩選器」為例
- 步驟6：點選「新增」按鈕
- 步驟7：在WMI查詢視窗，「查詢」欄位輸入  
SELECT \* FROM CIM\_DataFile WHERE path="\\Program Files\\Internet Explorer\\" AND filename="iexplore" AND extension="exe" AND version like "11.% "
- 步驟8：點選「確定」按鈕



# 常見問答(11/12)

- 步驟9：在新增WMI篩選器視窗，點選「儲存」按鈕，完成建立WMI篩選器
- 步驟10：點選IE11 GPO
- 步驟11：於「領域」標籤頁面移至最後，指定WMI篩選器
- 步驟12：點選「是」，將WMI篩選器連結至GPO



# 常見問答(12/12)

- 再次執行前述1 ~ 11的步驟建立IE 8的WMI篩選器
- IE 8與IE 11 WMI篩選器語法
  - IE 8 WMI篩選器 : `SELECT * FROM CIM_DataFile WHERE path="\\Program Files\\Internet Explorer\\" AND filename="iexplore" AND extension=".exe" AND version like "8.% "`
  - IE 11 WMI篩選器 : `SELECT * FROM CIM_DataFile WHERE path="\\Program Files\\Internet Explorer\\" AND filename="iexplore" AND extension=".exe" AND version like "11.% "`

# 政府組態基準(GCB)FAQ專區



- 行政院國家資通安全會報技術服務中心網站  
– <https://www.nccst.nat.gov.tw/GCB?lang=zh>

## 政府組態基準(GCB)-FAQ-作業系統專區

Windows 7

Windows 10

Windows Server 2008 R2

Windows Server 2012 R2

Red Hat Enterprise Linux 5

- 1.若UNC路徑未設定在「已強化的UNC路徑」清單中，是否會受此項組態設定影響？

如下圖所示，此項組態設定只會影響設定於「\\\*\SYSVOL」與「\\\*\NETLOGON」清單中之UNC路徑，其餘路徑不受影響。



- 2.是否需以Microsoft Windows Server 2016網域主機部署Microsoft Windows 10電腦政府組態基準(GCB)呢？

- 3.如何解決Windows Update自動更新造成使用者於登入時自動重新開機之狀況？

# 實作練習

NCCST



# 實作練習-環境說明

環境說明

- 本次採用AD環境進行實作練習
- 部署環境說明
  - VM名稱：7.Windows Server 2016(AD)
    - 帳號：Administrator；密碼：1qaz@WSX3edc
    - 組織單位(OU)：Training\_OU
  - VM名稱：8.Windows 10(Client)
    - 網域帳號：student；密碼：1qaz@WSX3edc
  - VM名稱：9.Windows 7(Client)
    - 網域帳號：student；密碼：1qaz@WSX3edc
- VM環境皆已安裝實作練習所需之軟體，包含Win10與Win7之GPO檔以及指令文字檔

# 實作練習1



## 實作說明

- Win7與Win10的使用者電腦皆放置於Training OU中，請使用AD部署Win7與Win10組態設定，並使用WMI篩選器自動判斷作業系統版本，進而套用專版GPO
- 執行步驟
  - 步驟1：將Win7與Win10 GPO匯入至AD中
  - 步驟2：建立Win7與Win10的WMI篩選器
  - 步驟3：將Win7 GPO連結Win7的WMI篩選器；Win10 GPO連結Win10的WMI篩選器
  - 步驟4：將Win7與Win10 GPO連結至組織單位
  - 步驟5：分別登入Win7與Win10 使用者電腦，使用gpupdate /force更新組態設定
  - 步驟6：使用rsop.msc或gpresult指令檢視部署結果

# 實作練習2(1/2)

實作說明

- 目前已知Win10有下列3項設定值須調整

項目	TWGCB-ID	項目名稱	設定值
1	TWGCB-01-005-0002	密碼最長使用期限	30
2	TWGCB-01-005-0165	系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章	停用
3	TWGCB-01-005-0245	記錄檔大小上限(KB)-安全性	啟用： 204800(KB)

- 請於AD內，建立名為「Win10例外管理」之GPO，於GPO內設定上述項目，部署至Win10之使用者電腦

# 實作練習2(2/2)



## 實作說明

- 執行步驟

- 步驟1：建立名為「Win10例外管理」之GPO
- 步驟2：於「Win10例外管理」GPO內設定此3項組態項目
- 步驟3：建立Win10的WMI篩選器
- 步驟4：將「Win10例外管理」GPO連結至Win10的WMI篩選器
- 步驟5：將「Win10例外管理」GPO連結至組織單位
- 步驟6：將「Win10例外管理」GPO順序調至第一位
- 步驟7：登入Win10 使用者電腦，使用gpupdate /force 更新組態設定
- 步驟8：使用rsop.msc或gpresult指令檢視部署結果

報告完畢  
敬請指教

NCCST