政府組態基準(GCB)實作研習活動
Windows 10派送說明

行政院國家資通安全會報技術服務中心

大綱

- 群組原則介紹
- GCB導入流程
  - 使用AD導入GCB
  - 使用單機導入GCB
- 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
- 問題與討論

群組原則介紹

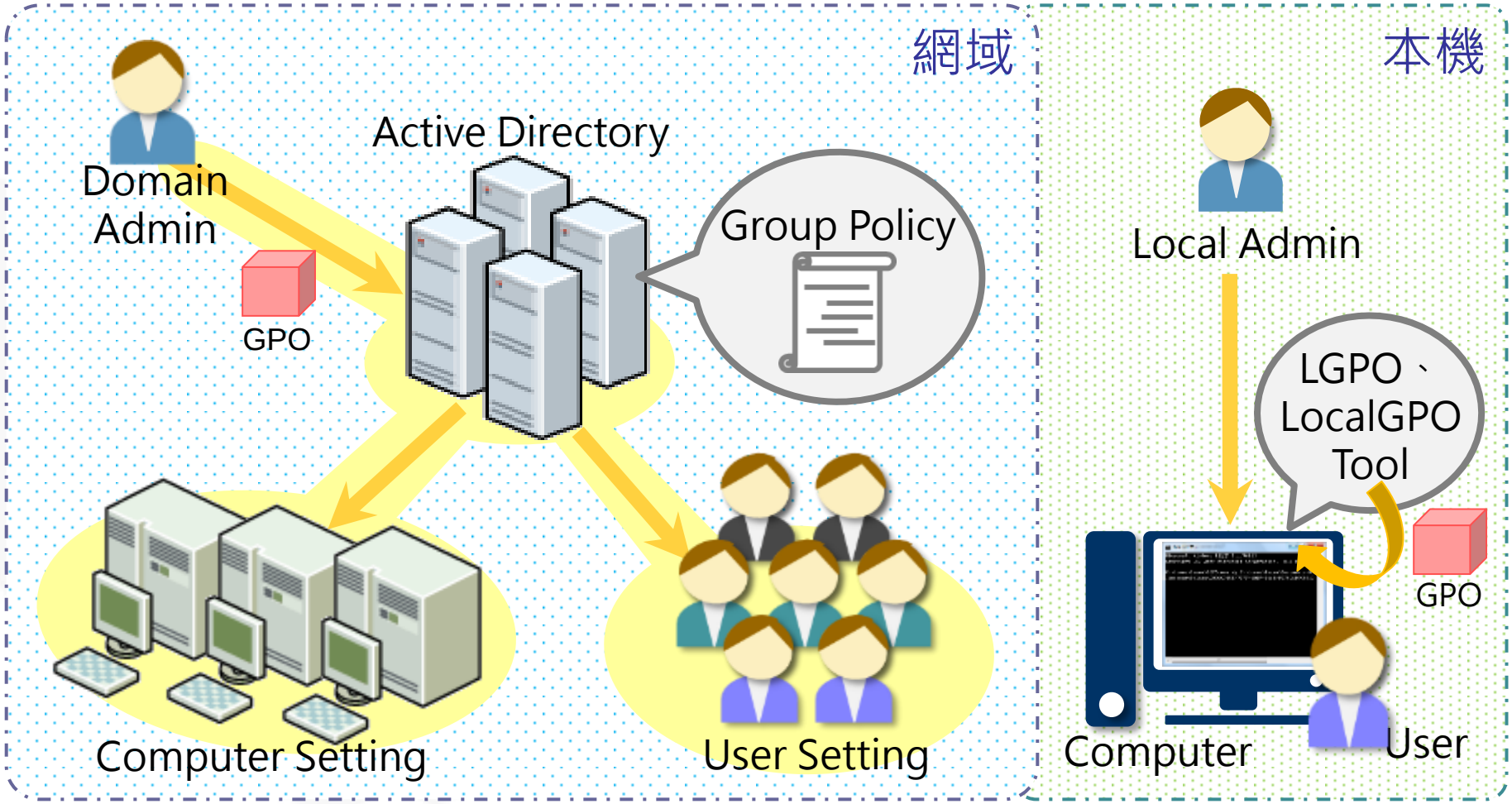
何謂群組原則(1/2)

- 群組原則：
  - –組織在電腦上強制套用設定的方式
- 目的：

參考資料 : https://technet.microsoft.com/zh-tw/library/hh147307(v=ws.10).aspx

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



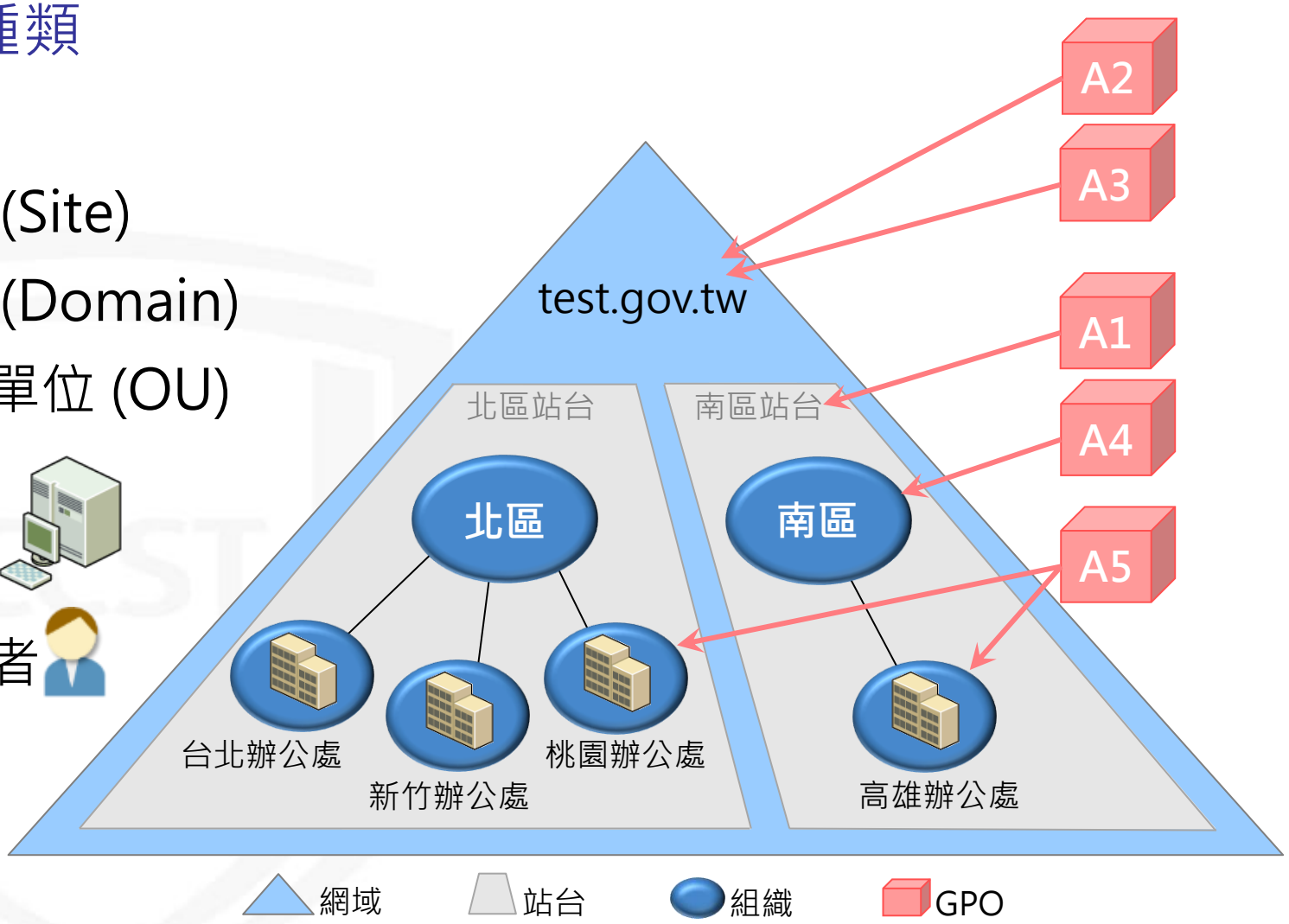
Active Directory網域介紹

- Active Directory(簡稱AD)
  - Microsoft提出在Windows Server上的目錄服務，可儲存所有網路資源(如電腦、印表機或使用者等)相關資訊，並且易於存取

1. 集中管理使用者的帳戶資訊
2. 擔任第一層的身分安全驗證伺服器
3. 集中維護網域內的共用資源
4. 配置各階層組織單位，給予不同原則限制

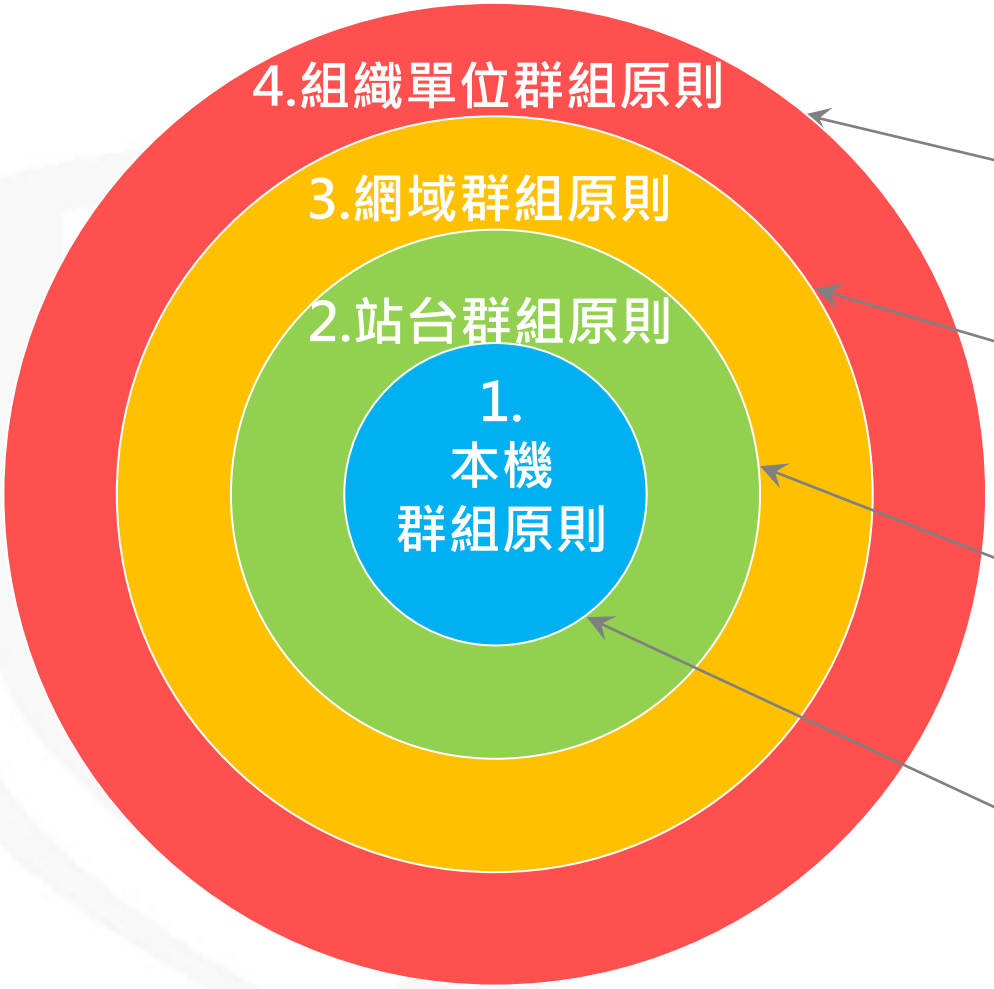
群組原則的關聯對象

- 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

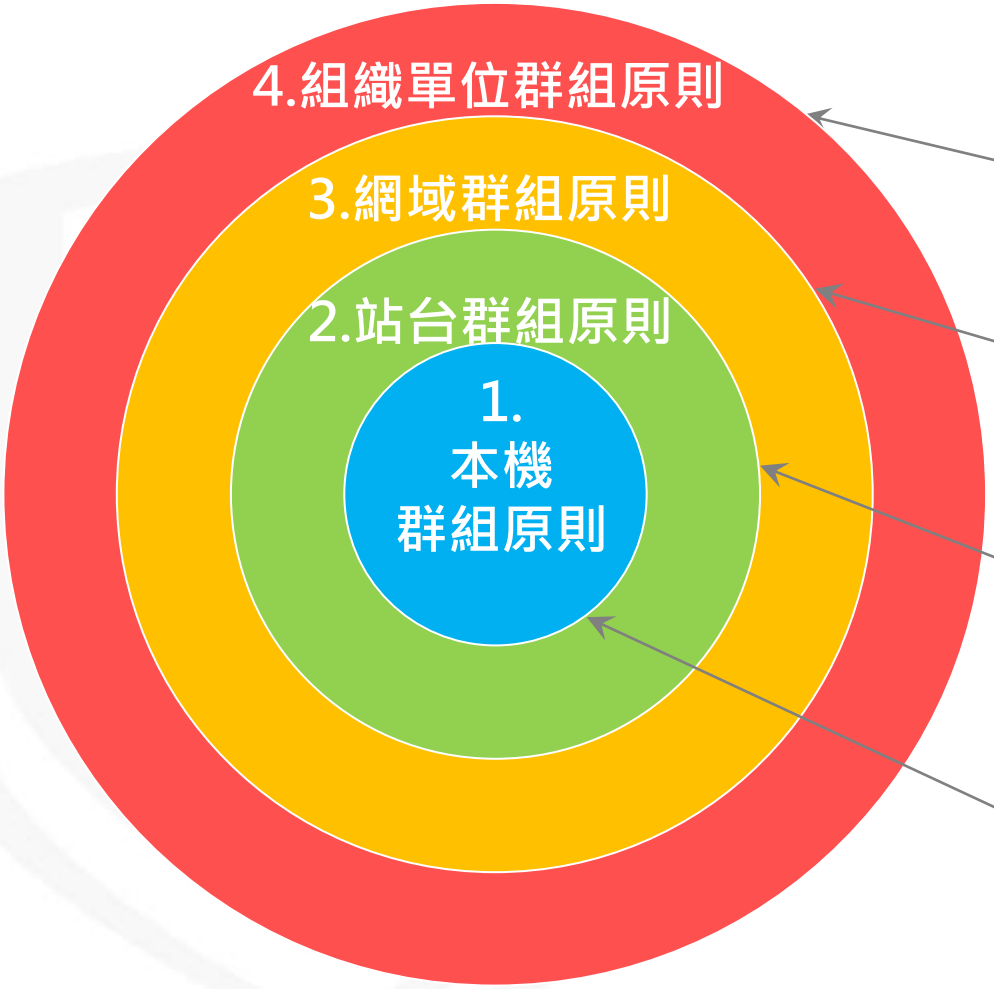
專委：
- 午休時間一個小時
- 下班時間下午五點半

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



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

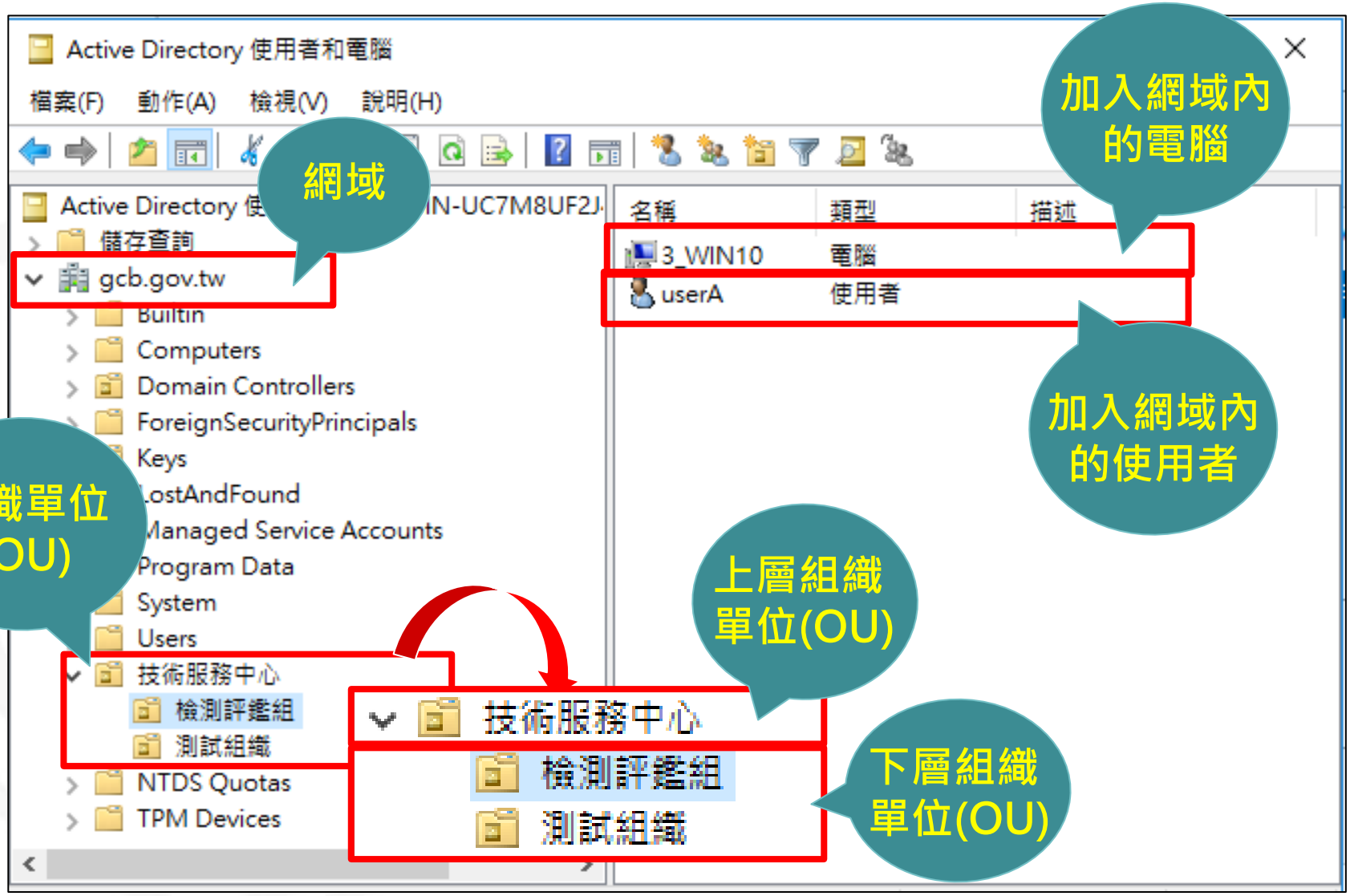
強制(禁止覆蓋)

- 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

內容組成	GPO	
	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


Active Directory 使用者和電腦
檔案(F) 動作(A) 檢視(V) 說明(H)
網域
加入網域內的電腦
加入網域內的使用者
組織單位(OU)
上層組織單位(OU)
下層組織單位(OU)
Active Directory 使
儲存查詢
gcb.gov.tw
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
技術服務中心
檢測評鑑組
測試組織
NTDS Quotas
TPM Devices
名稱
類型
描述
3_WIN10
電腦
userA
使用者

有獎徵答

有獎徵答1-題目

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

本機群組原則

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

本機：
- 密碼到期**5天前提示**

gcb.gov.tw網域：
- 密碼到期**12天前提示**

技術服務中心：
- 密碼到期**10天前提示**

主任室：
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期**3天前提示**

有獎徵答1-解答

主任室密碼到期提示時間=10天前

檢測評鑑組密碼到期提示時間=3天前

套用順序

本機群組原則

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

本機：
- 密碼到期**5天前提示**

gcb.gov.tw網域：
- 密碼到期**12天前提示**

技術服務中心：
- 密碼到期**10天前提示**

主任室：
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期**3天前提示**

有獎徵答2-題目

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

本機群組原則

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

本機：
- 密碼到期**5天前提示**

gcb.gov.tw網域：
- 密碼到期**12天前提示**

技術服務中心：
- 密碼到期**10天前提示**

主任室：**禁止繼承**
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期**3天前提示**

有獎徵答2-解答

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=3天前

套用順序

1. 本機群組原則
2. 站台群組原則
3. 網域群組原則
4. 上層組織單位群組原則
5. 下層組織單位群組原則

本機：
- 密碼到期**5天前提示**

gcb.gov.tw網域：
- 密碼到期**12天前提示**

技術服務中心：
- 密碼到期**10天前提示**

主任室：**禁止繼承**
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期**3天前提示**

有獎徵答3-題目

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

本機群組原則

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

本機：
- 密碼到期5天前提示

gcb.gov.tw網域：強制
- 密碼到期12天前提示

技術服務中心：
- 密碼到期10天前提示

主任室：禁止繼承
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期3天前提示

有獎徵答3-解答

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=12天前

套用順序

本機群組原則

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

本機：
- 密碼到期**5天前提示**

gcb.gov.tw網域：**強制**
- 密碼到期**12天前提示**

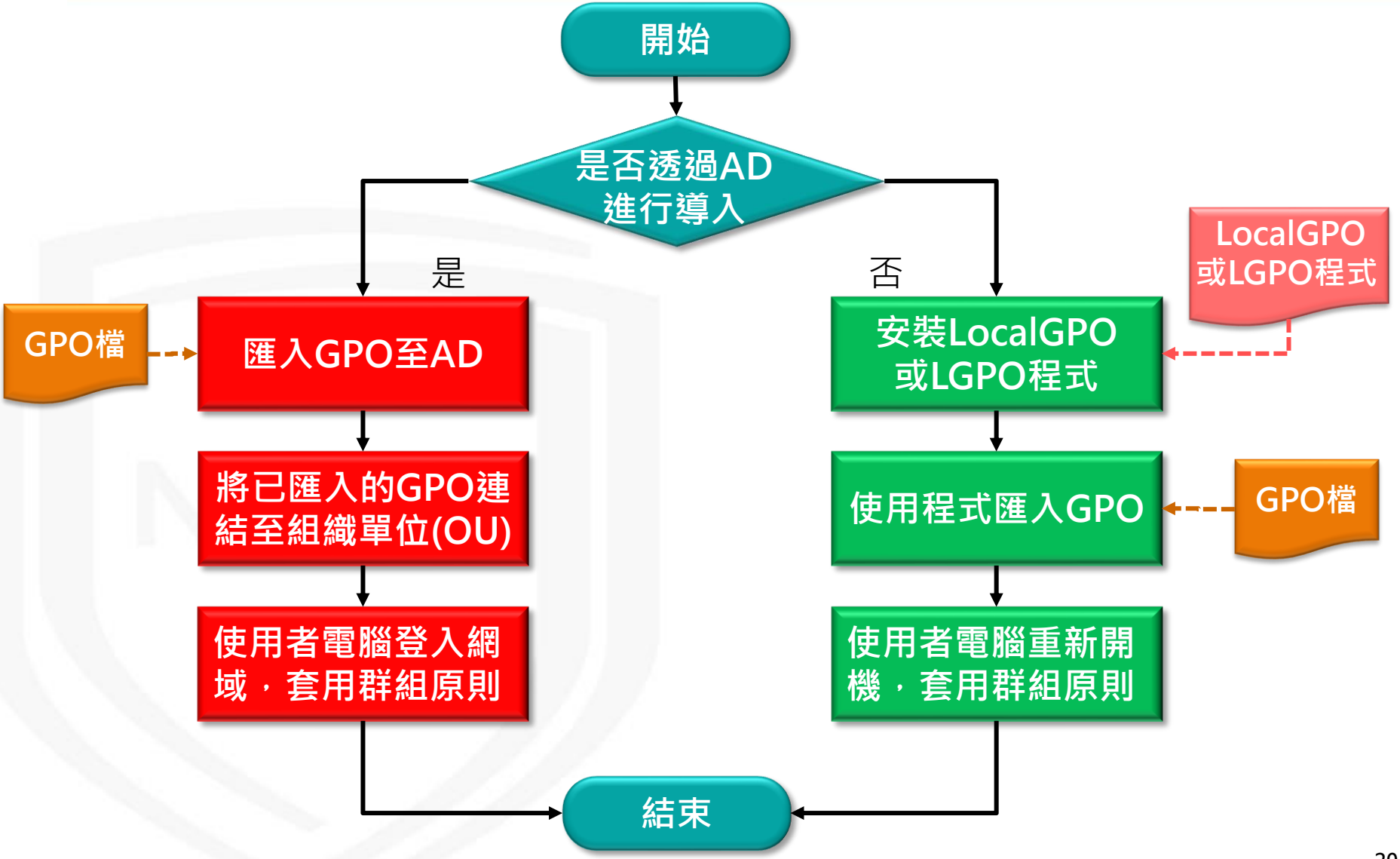
技術服務中心：
- 密碼到期**10天前提示**

主任室：**禁止繼承**
- **無密碼到期提示**

檢測評鑑組：
- 密碼到期**3天前提示**

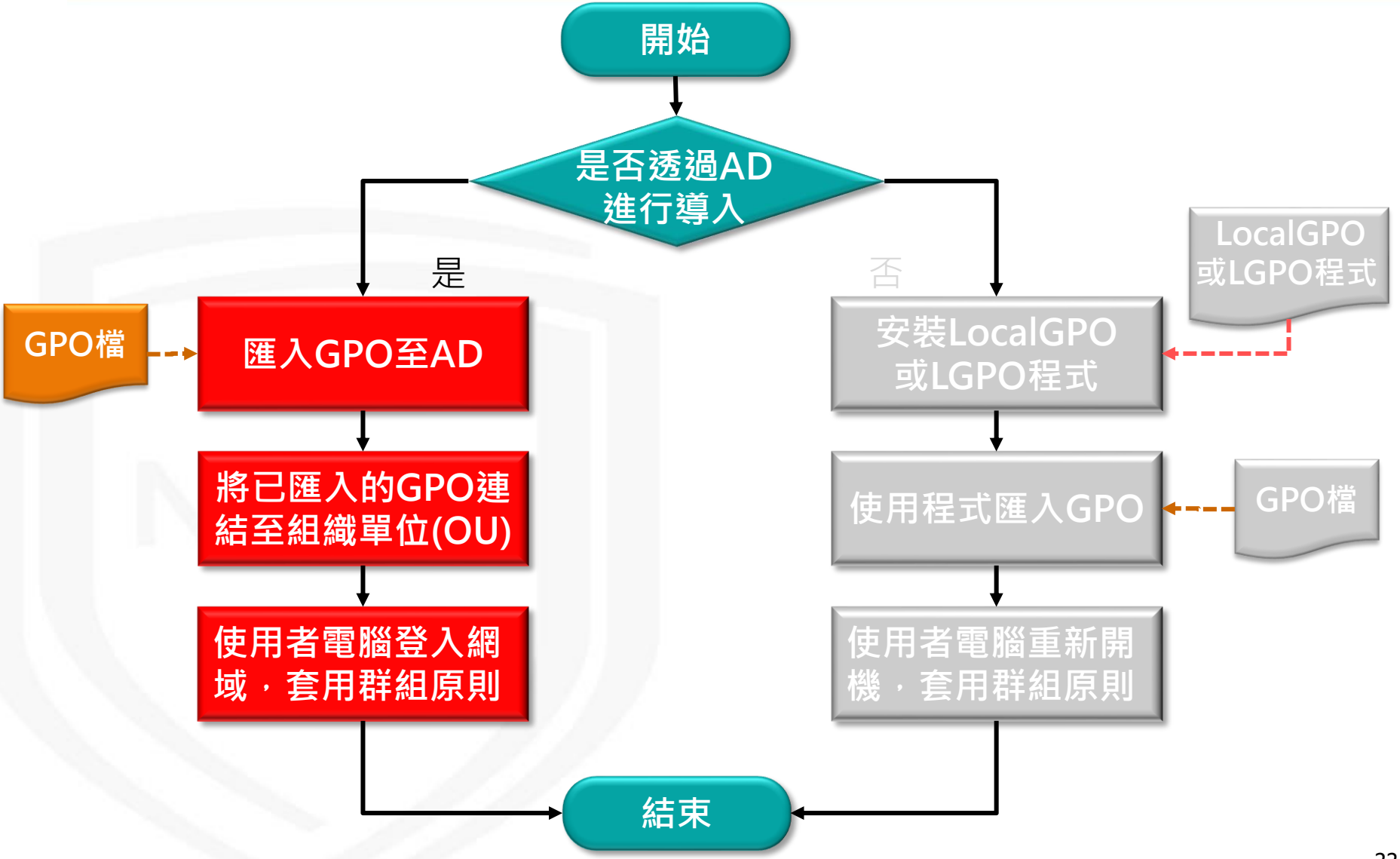
GCB導入流程

GCB導入流程


開始
是否透過AD進行導入
是
否
GPO檔
匯入GPO至AD
將已匯入的GPO連結至組織單位(OU)
使用者電腦登入網域，套用群組原則
LocalGPO或LGPO程式
安裝LocalGPO或LGPO程式
使用程式匯入GPO
GPO檔
使用者電腦重新開機，套用群組原則
結束

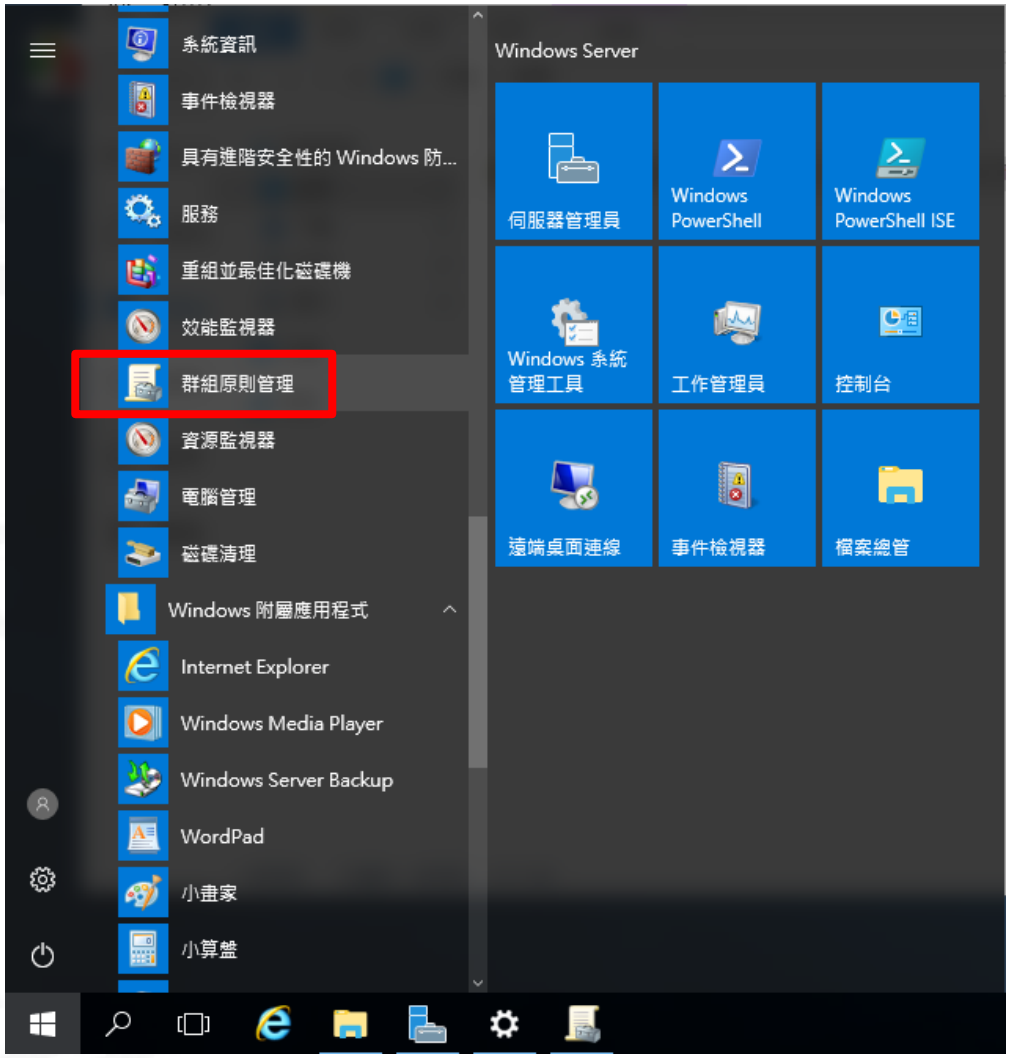
使用AD導入GCB

GCB導入流程


開始
是否透過AD進行導入
是
否
GPO檔
匯入GPO至AD
將已匯入的GPO連結至組織單位(OU)
使用者電腦登入網域，套用群組原則
LocalGPO或LGPO程式
安裝LocalGPO或LGPO程式
使用程式匯入GPO
GPO檔
使用者電腦重新開機，套用群組原則
結束

匯入GPO至AD(1/6)

- 點擊開始→所有程式→群組原則管理

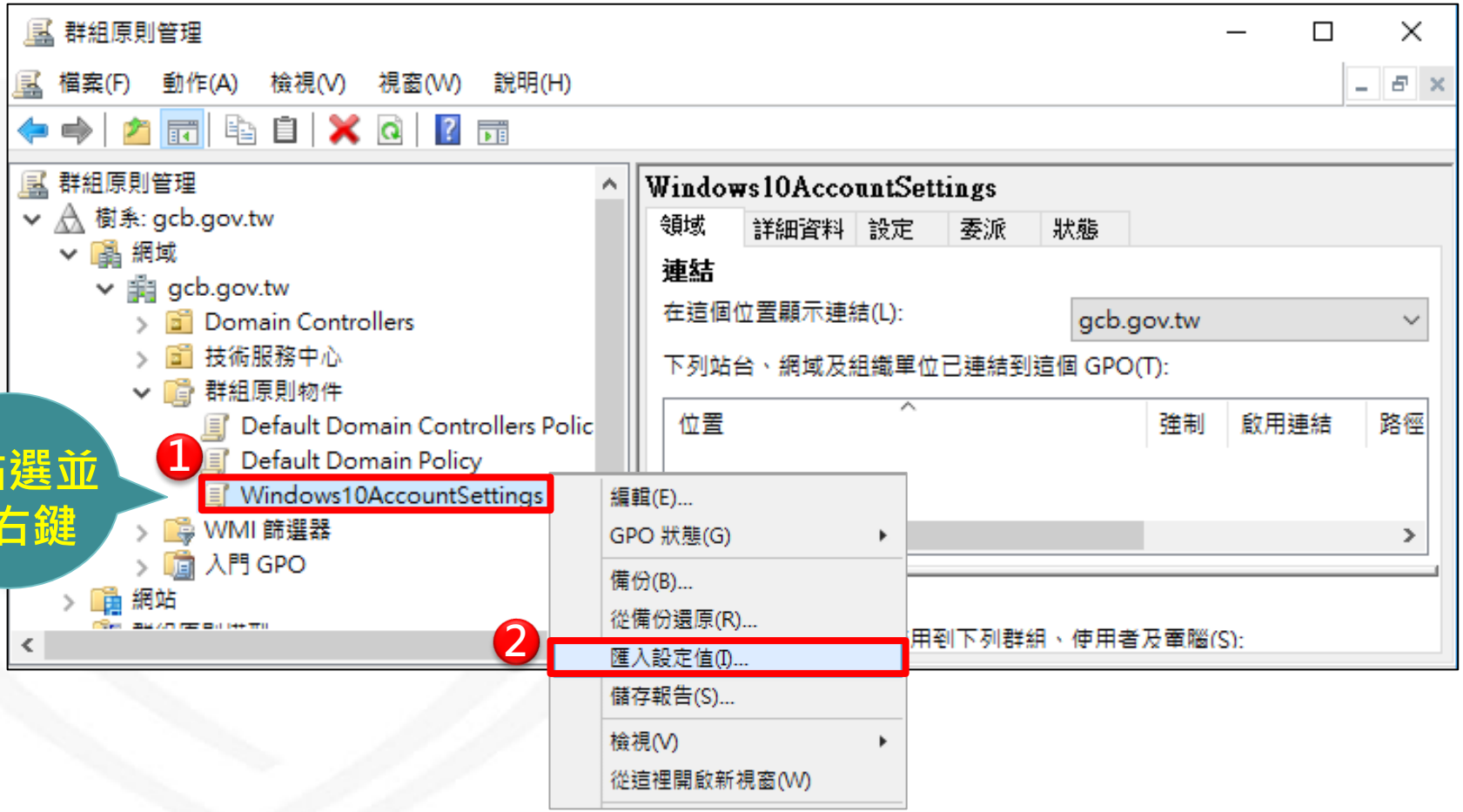


匯入GPO至AD(2/6)

- 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

匯入GPO至AD(3/6)

- 點選新建的群組原則物件按滑鼠右鍵→選擇「匯入設定值」



匯入GPO至AD(4/6)

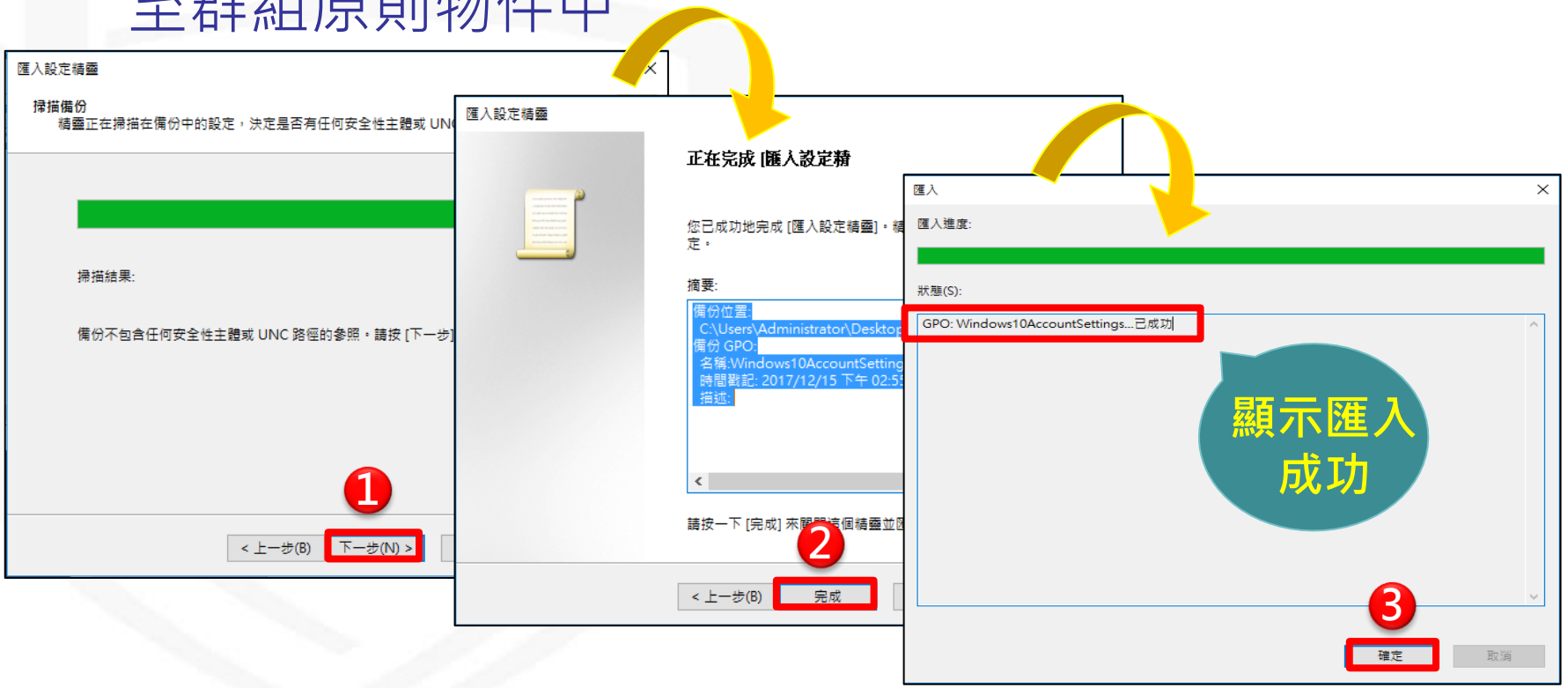
- 在歡迎使用【匯入設定精靈】頁面→點選「下一步」
- 在備份GPO頁面→點選「下一步」

匯入GPO至AD(5/6)

- 在備份位置頁面→選取放置GPO的資料夾→點選「下一步」
- 在來源GPO頁面→選取欲匯入的GPO→點選「下一步」

匯入GPO至AD(6/6)

- 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

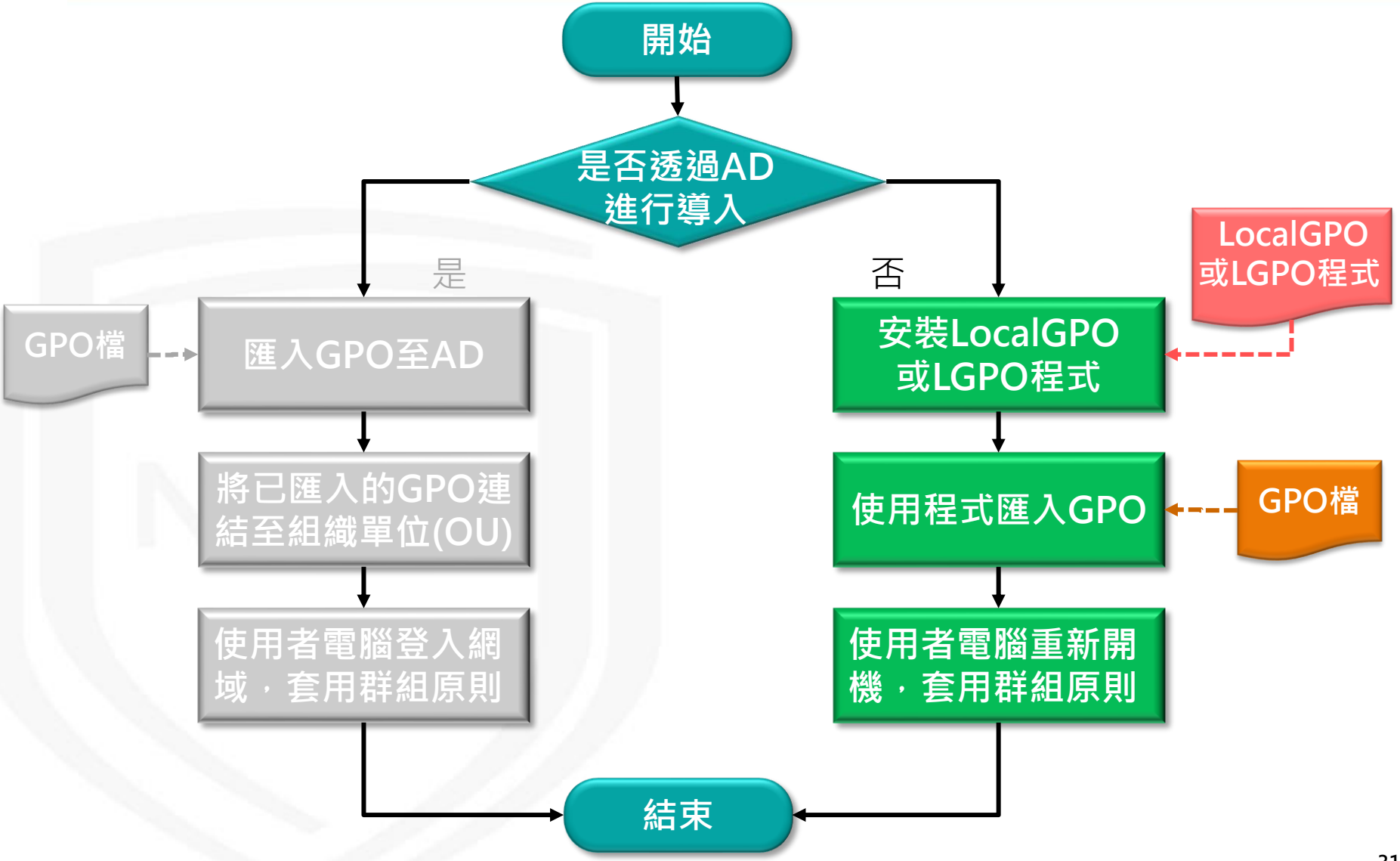


將GPO連結至組織單位(OU)

- 將已匯入GPO的群組原則物件拖曳至組織單位(OU)，完成部署作業
- 使用者重新開機或使用gpupdate /force指令更新組態，即可套用GCB設定

使用單機導入GCB

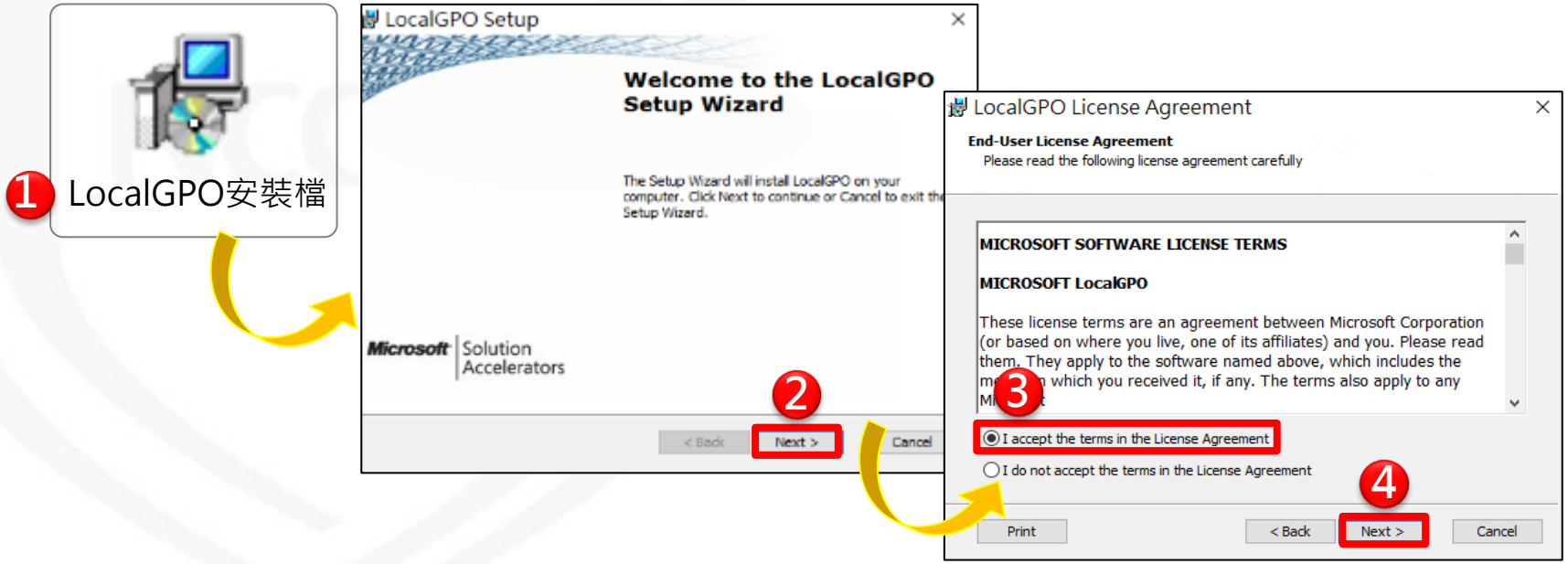
GCB導入流程


開始
是否透過AD進行導入
是
否
GPO檔
匯入GPO至AD
將已匯入的GPO連結至組織單位(OU)
使用者電腦登入網域，套用群組原則
LocalGPO或LGPO程式
安裝LocalGPO或LGPO程式
使用程式匯入GPO
GPO檔
使用者電腦重新開機，套用群組原則
結束

使用LocalGPO程式導入GCB

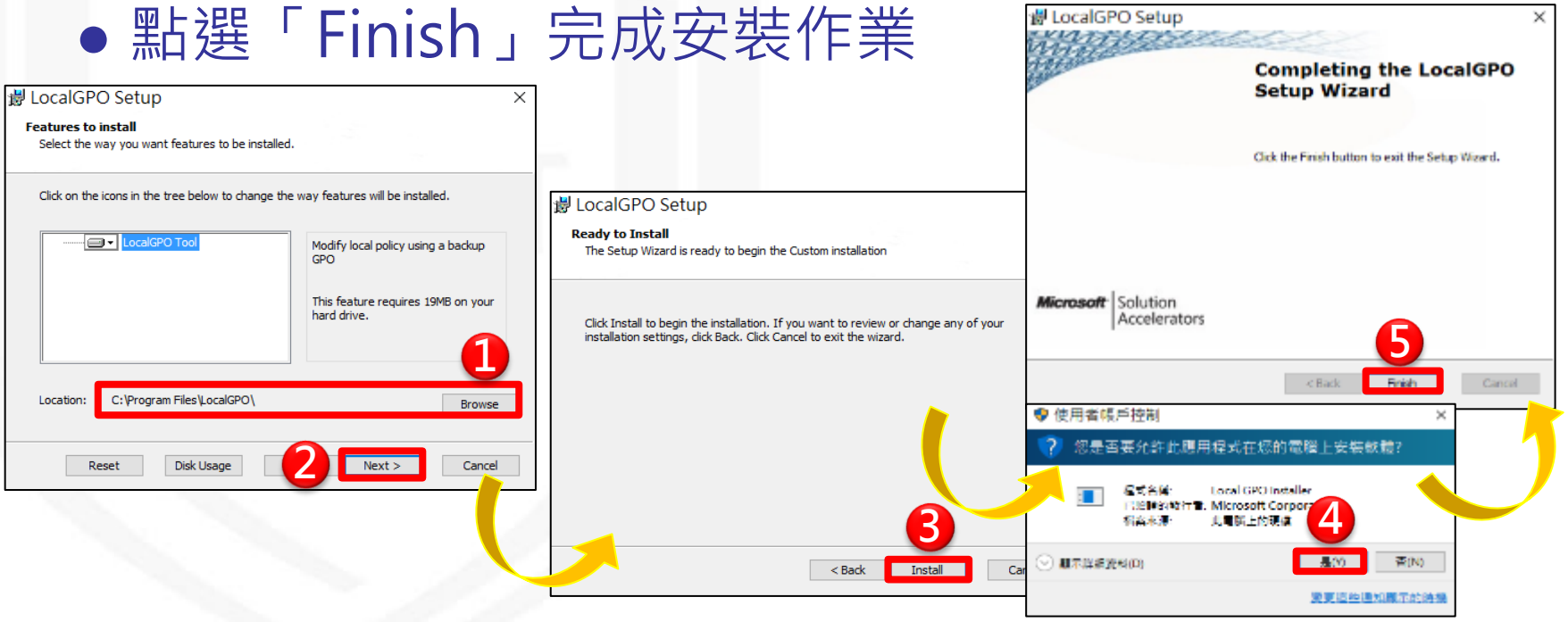
安裝LocalGPO程式(1/2)

- 執行「LocalGPO」安裝檔
- 在Welcome to the LocalGPO Setup Wizard頁面→點選「Next」
- 在End-User License Agreement頁面→勾選接受授權協議→點選「Next」



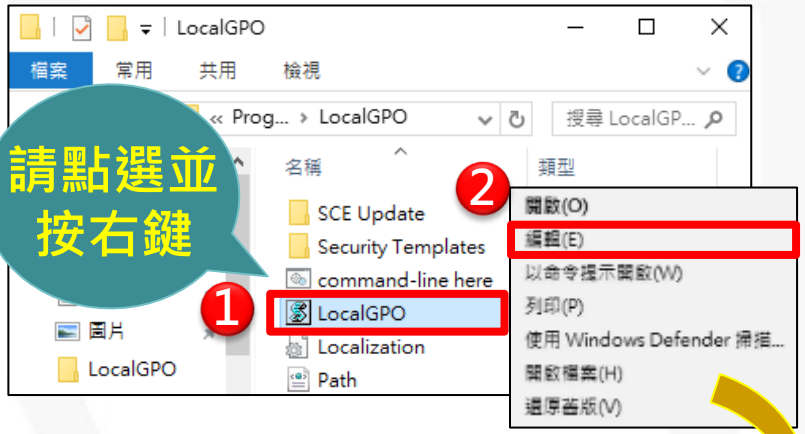
安裝LocalGPO程式(2/2)

- 在Features to Install頁面→確認安裝路徑→點選「Next」
- 在Ready to Install頁面→點選「Install」進行安裝
- 點選「是」，允許安裝LocalGPO在這部電腦上
- 點選「Finish」完成安裝作業



使用LocalGPO程式匯入GPO(1/4)

- 至LocalGPO安裝資料夾路徑(C:\Program Files\LocalGPO) →找到LocalGPO.wsf檔案→點選右鍵→選擇「編輯」
- 搜尋「Sub ChkOSVersion」找到下圖程式碼位置




```
    '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 =
       strOS = "XP"
    Else
      strMessage = DisplayMessage(conLABEL_CODE002)
      Call MsgBox(strMessage, vbOKOnly + vbCritical, strTi
      Call CleanupandExit
    End If

End Sub
```

找到此段程式碼

使用LocalGPO程式匯入GPO(2/4)

- 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 _
    '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(strOpVe
       strOS = "Win8"
    ElseIf(Left(strOpVe
       strOS = "WS08R2"
    ElseIf(Left(strOpVe
       strOS = "Win7"
    ElseIf(Left(strOpVe
       strOS = "WS08"
    ElseIf(Left(strOpVe
       strOS = "VISTA"
    ElseIf(Left(strOpVe
       strOS = "WS03"
    ElseIf(Left(strOpVe
       strOS = "XP"
    ElseIf(Left(strOpVer,3) = "5.1") and (st roductType = "1") then
       strOS = "XP"
    Else
      'strMessage = DisplayMessage(conLABEL_CODE002)
      'Call MsgBox(strMessage, vbOKOnly + vbCritical, strTitle)
      'Call CleanupandExit
       strOS = "Win8"
    End If

End Sub
```

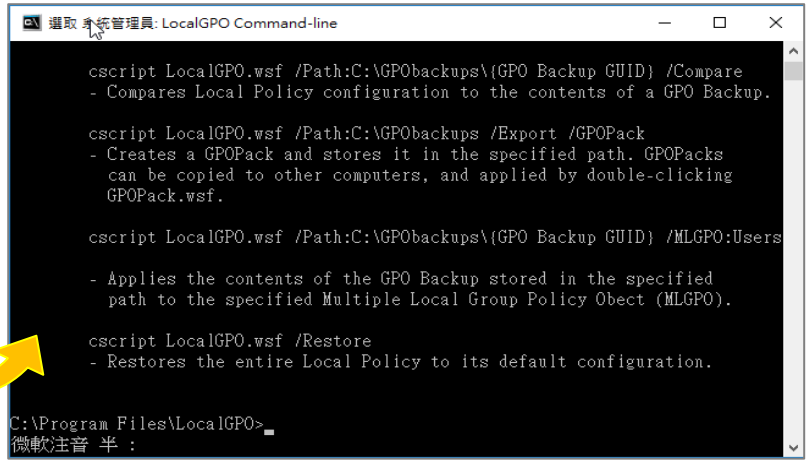
- 修改說明：
  請將前三行變成註解，並新增最後一行程式碼

```
'strMessage = DisplayMessage(conLABEL_CODE002)
'Call MsgBox(strMessage, vbOKOnly + vbCritical, strTitle)
'Call CleanupandExit
strOS = "Win8"
```

請依紅字標示修改

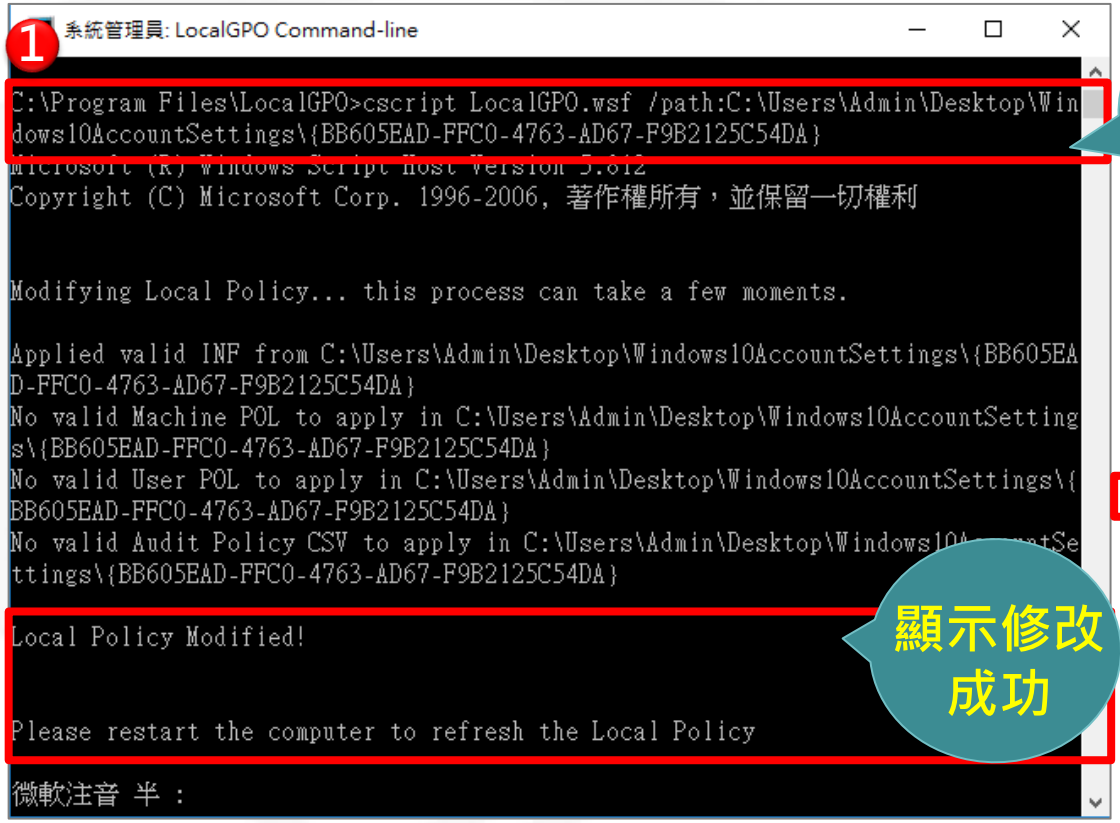
使用LocalGPO程式匯入GPO(3/4)

- 點選「LocalGPO Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
- 複製GPO所在的完整目錄路徑



使用LocalGPO程式匯入GPO(4/4)

- 於「LocalGPO Command-line」輸入語法
  - –cscript LocalGPO.wsf /path:"<放置GPO的完整目錄路徑>"
- 重新開機或使用gpupdate /force指令更新組態



輸入語法與路徑

路徑不能有空白

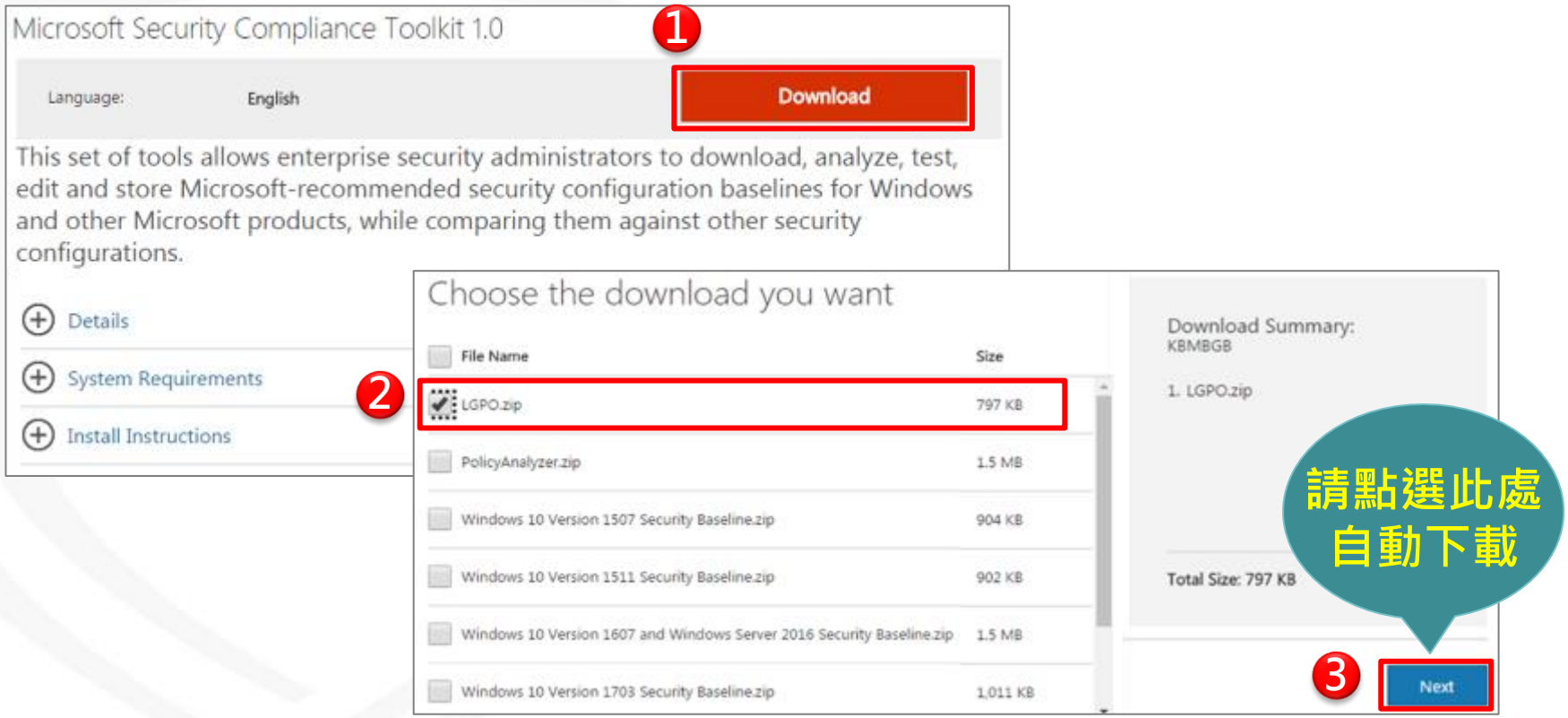
顯示修改成功

輸入語法更新或重開機

使用LGPO程式導入GCB

使用LGPO程式匯入GPO(1/3)

- 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

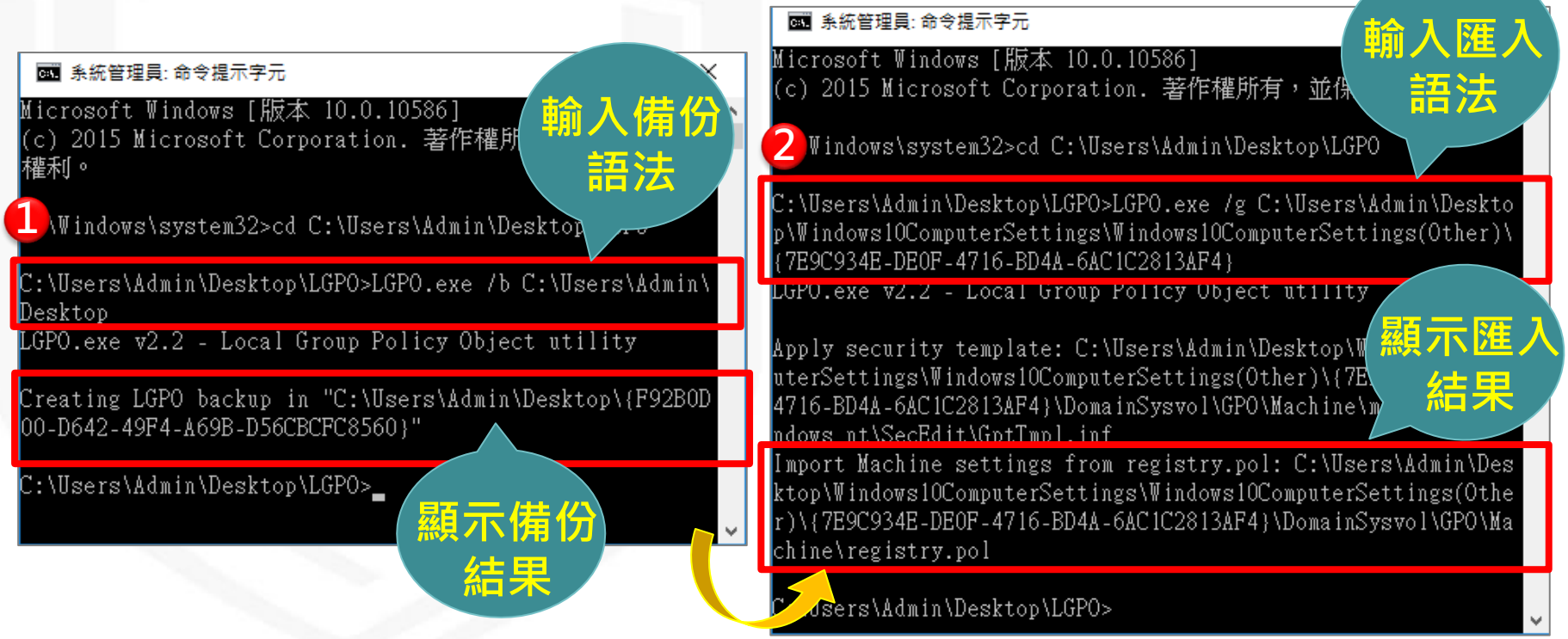


使用LGPO程式匯入GPO(2/3)

- 點選「Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
- 於「Command-line」輸入語法切換LGPO目錄
  –cd<放置LGPO解壓縮後的完整目錄路徑>

使用LGPO程式匯入GPO(3/3)

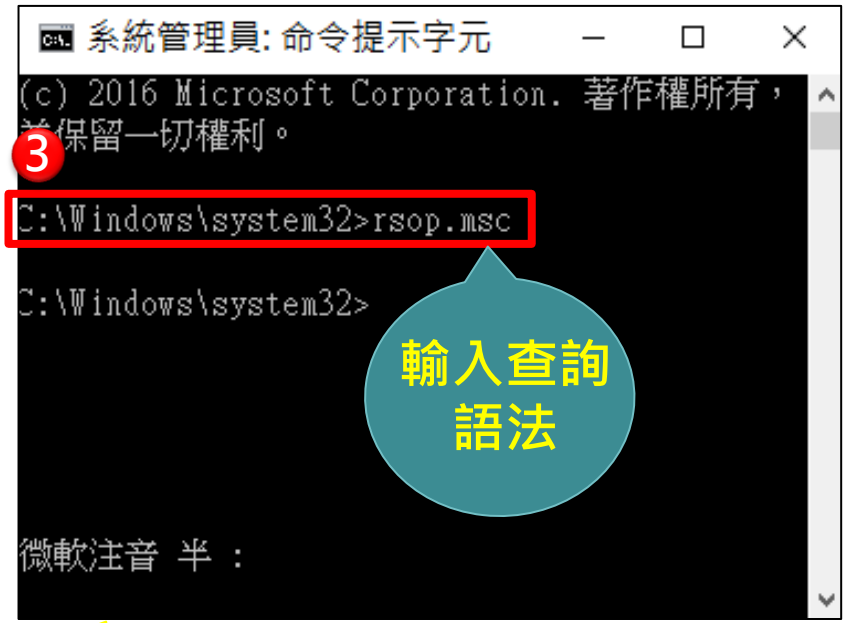
- 於「Command-line」輸入語法:
  - LGPO.exe /b **<絕對路徑>**備份電腦原始組態設定
  - LGPO.exe /g **<絕對路徑>** 將GPO檔案匯入電腦
- 重新開機或使用gpupdate /force指令更新組態



檢查GPO套用狀況之方式

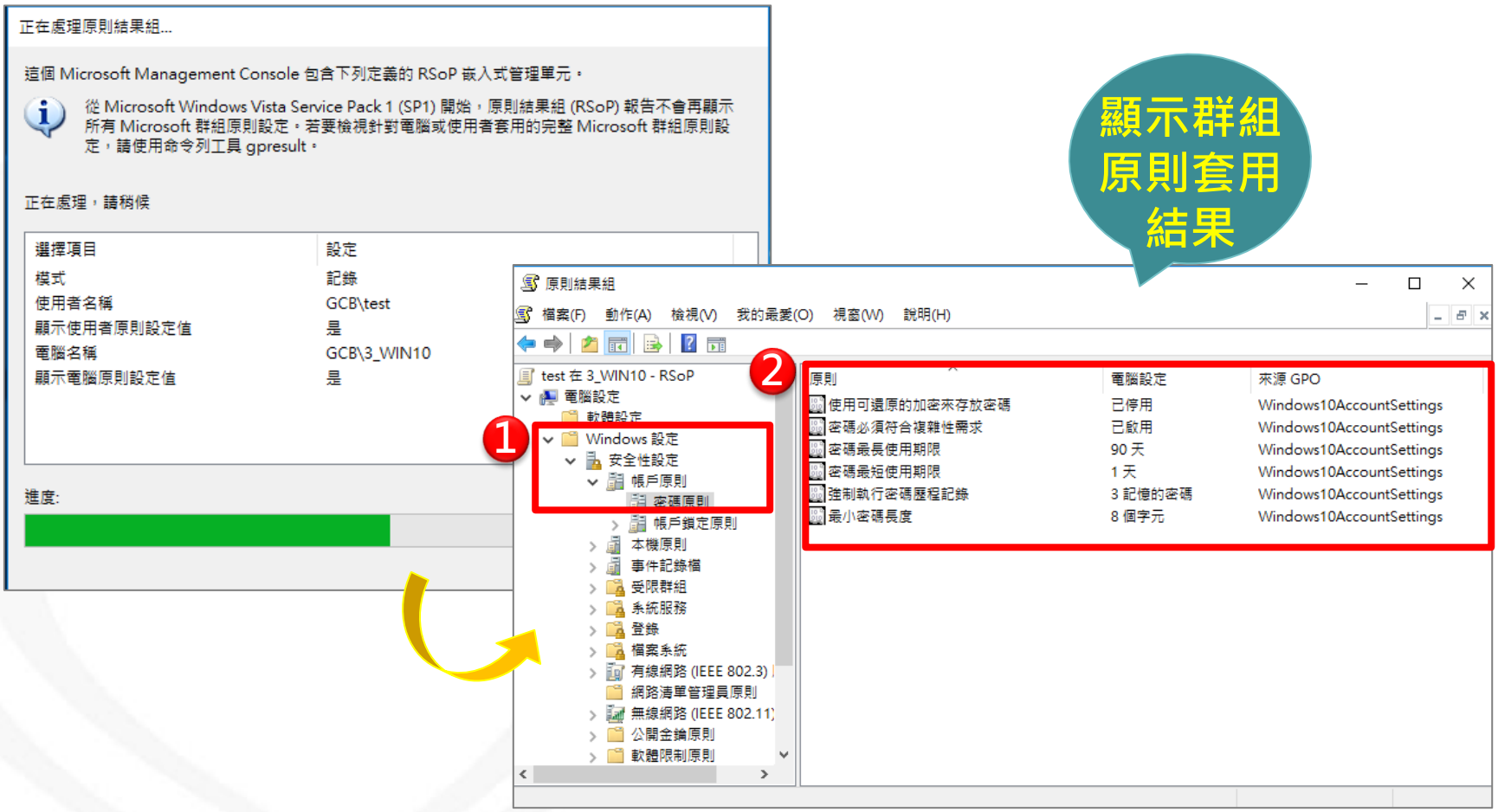
AD環境下的檢查方式(1/4)

- 使用RSOP檢查群組原則
  - –點選「Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - –於「Command-line」輸入Rsop.msc查詢群組原則結果



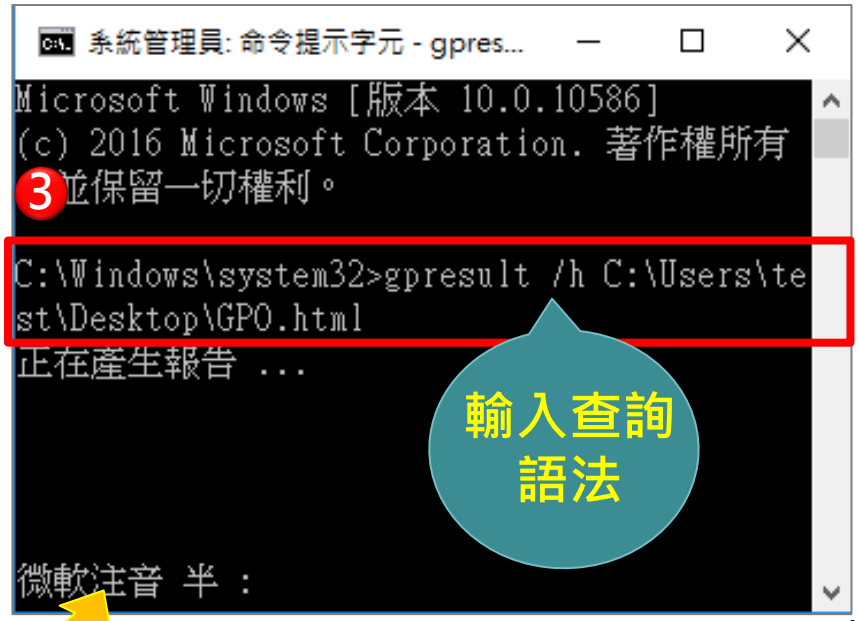
AD環境下的檢查方式(2/4)

- 使用RSOP檢查群組原則，顯示如下



AD環境下的檢查方式(3/4)

- 使用Gpresult檢查群組原則
  - 點選「Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - 於「Command-line」輸入gpresult /h <檔案儲存路徑>\檔名.html

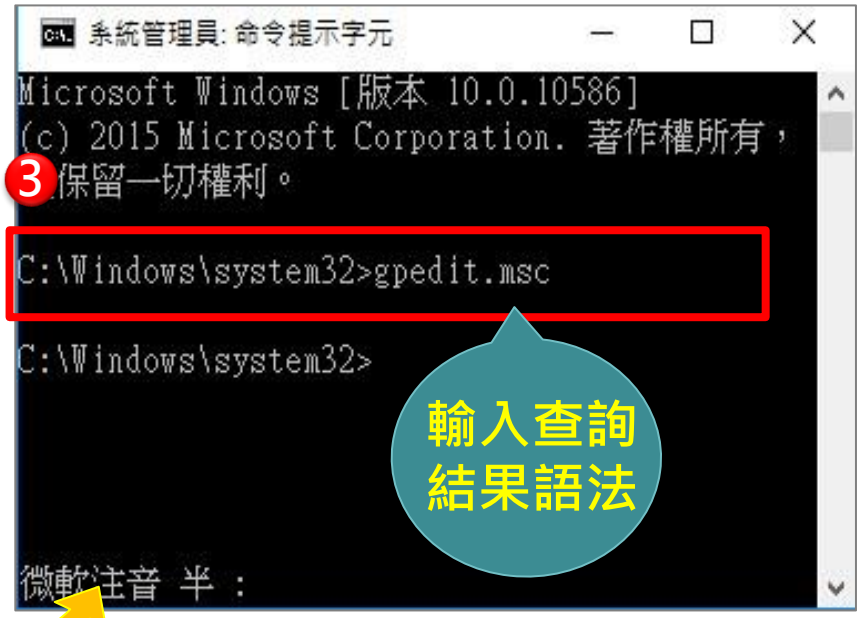


AD環境下的檢查方式(4/4)

- 使用Gpresult檢查群組原則，顯示如下

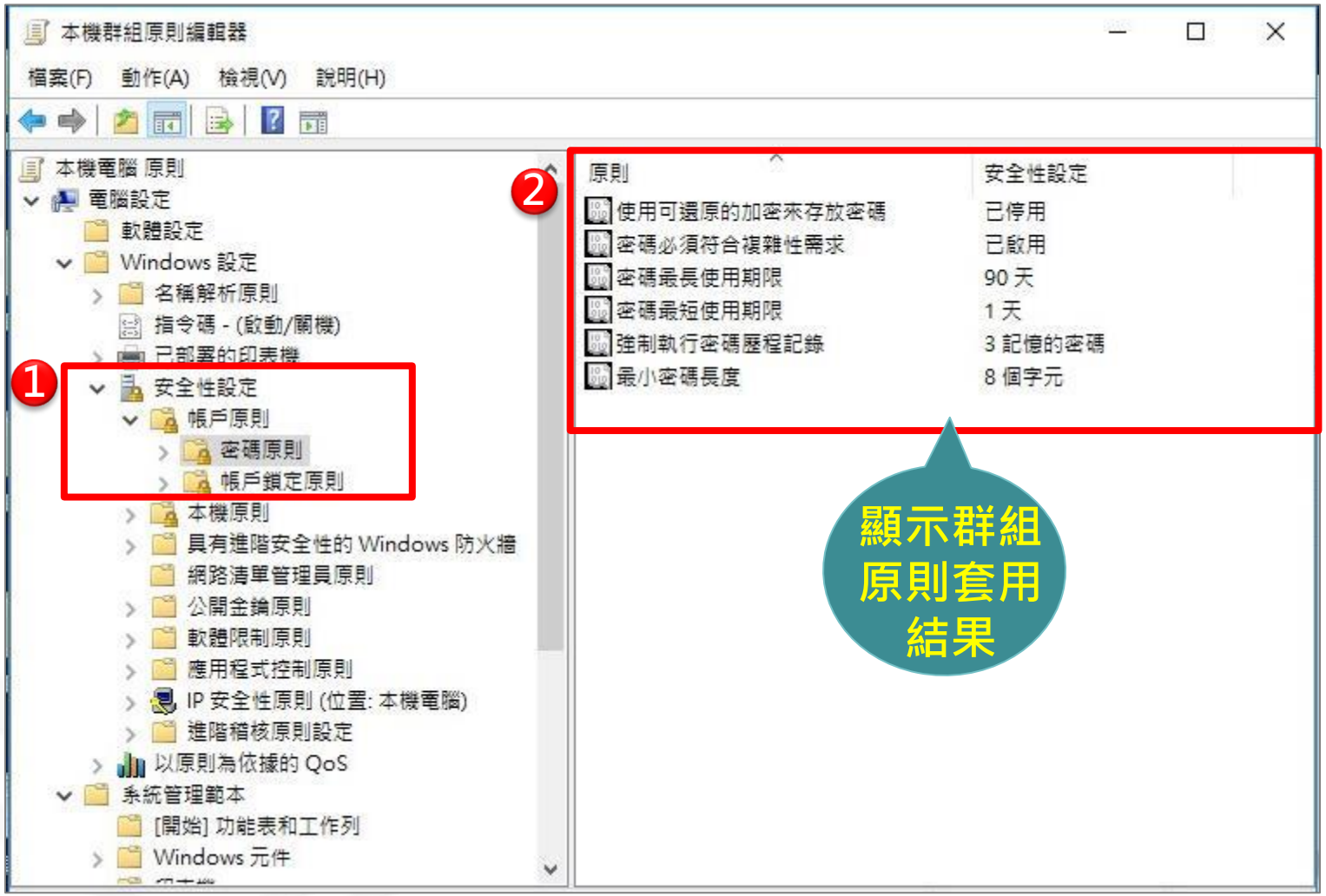
單機環境下的檢查方式(1/2)

- 使用Gpedit.msc檢查群組原則
  - –點選「Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - –於「Command-line」輸入Gpedit.msc



單機環境下的檢查方式(2/2)

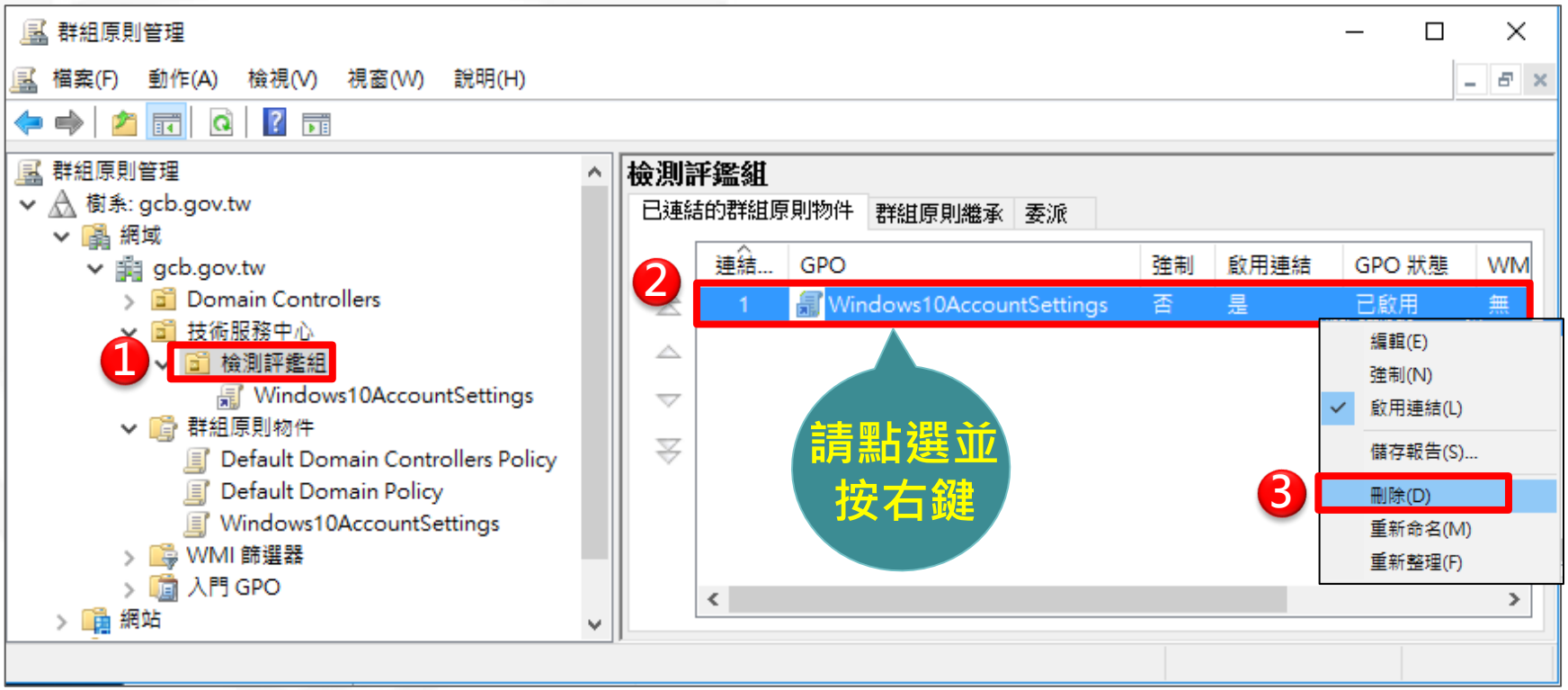
- 使用Gpedit.msc檢查群組原則，顯示如下



恢復原始設定之方式

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

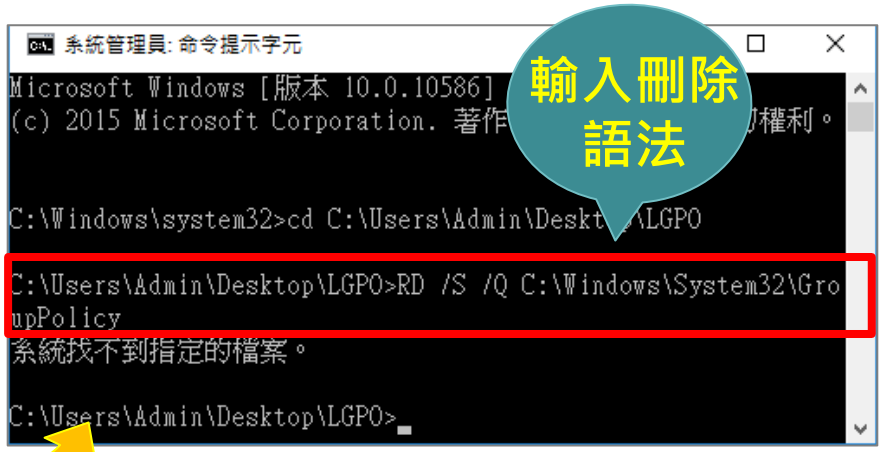


單機環境下恢復原始設定方式(1/2)

- 使用LocalGPO恢復原始設定
  - 點選「LocalGPO Command-line」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - 執行cscript LocalGPO.wsf /Restore
  - 重新開機或使用gpupdate /force指令更新組態

單機環境下恢復原始設定方式(2/2)

- 使用LGPO恢復原始設定
  - 點選「Command-line」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
  - 執行LGPO.exe /g <絕對路徑>，匯入原始備份的GPO檔案
  - 重新開機或使用gpupdate /force指令更新組態



例外管理調整GCB設定值

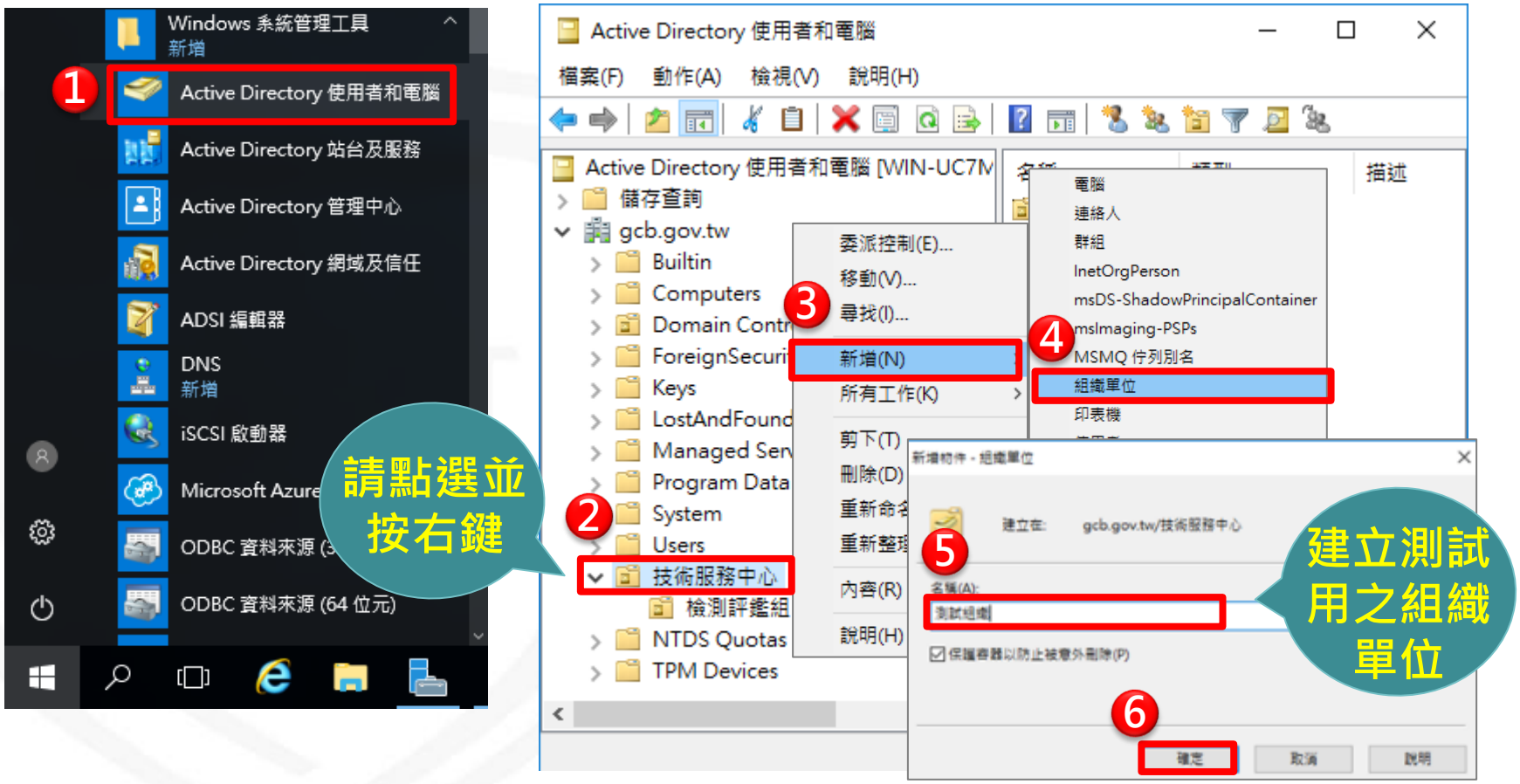
例外管理

- 套用GCB後，若發生系統異常或無法使用導致影響日常公務，則可以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

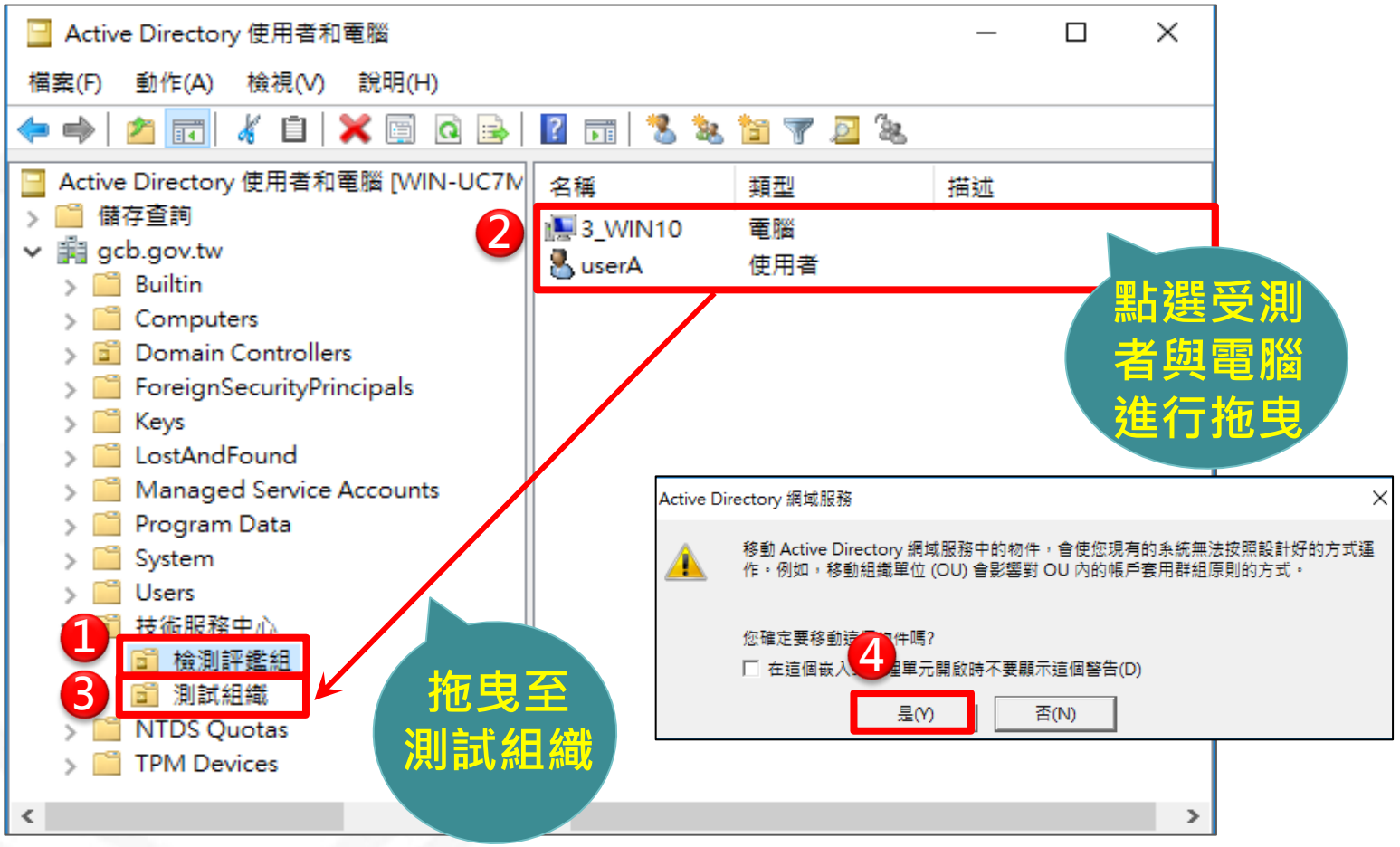
AD環境下調整與測試GCB(1/11)

- 點擊開始→所有程式→Active Directory使用者和電腦
- 建立測試組織單位(OU)



AD環境下調整與測試GCB(2/11)

- 拖曳受測使用者與電腦至剛建立的測試組織單位(OU)

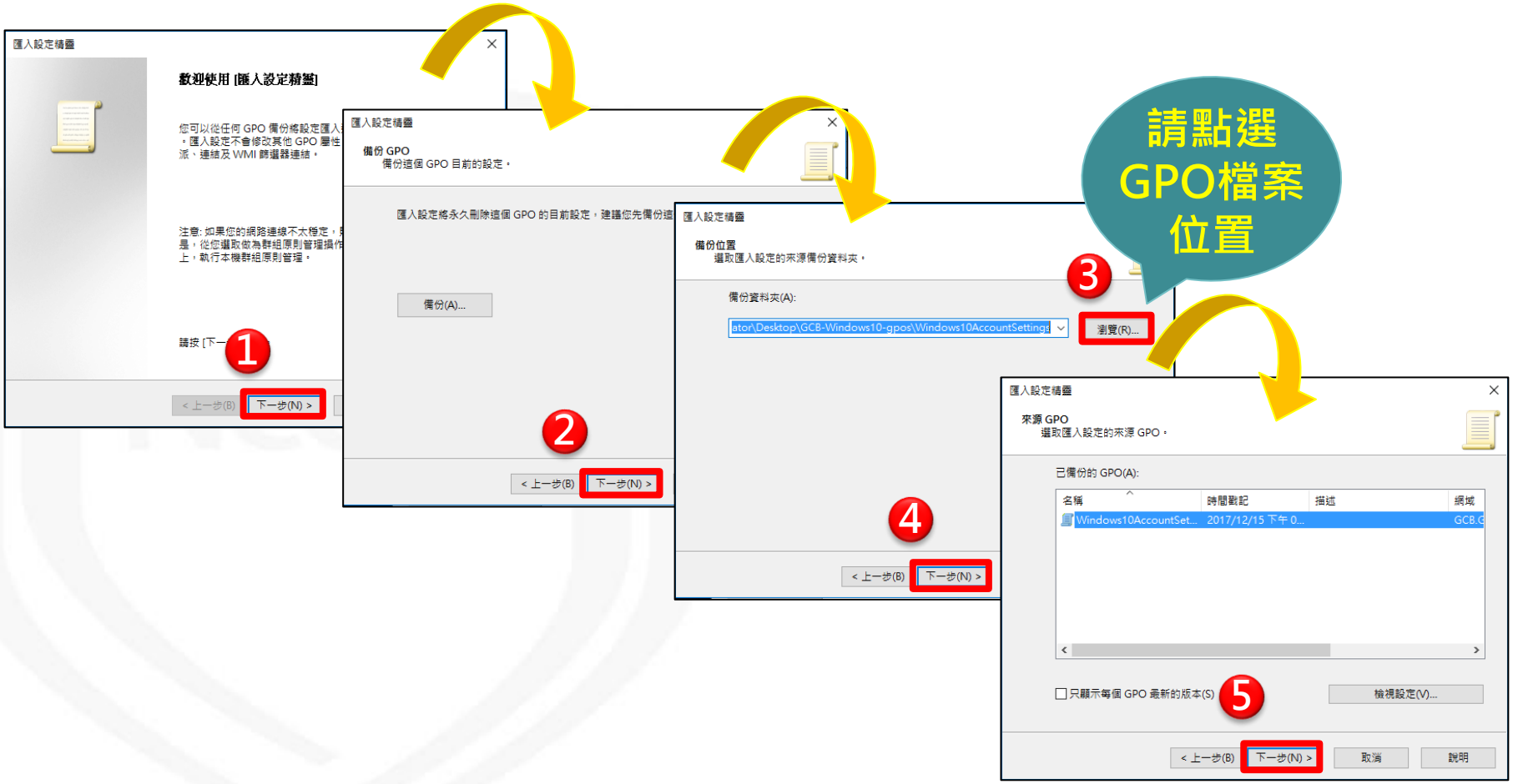


AD環境下調整與測試GCB(3/11)

- 建立測試的GPO
  - –在群組原則物件節點按滑鼠右鍵→選擇「新增」
  - –在「名稱」欄位→輸入測試的群組原則物件名稱

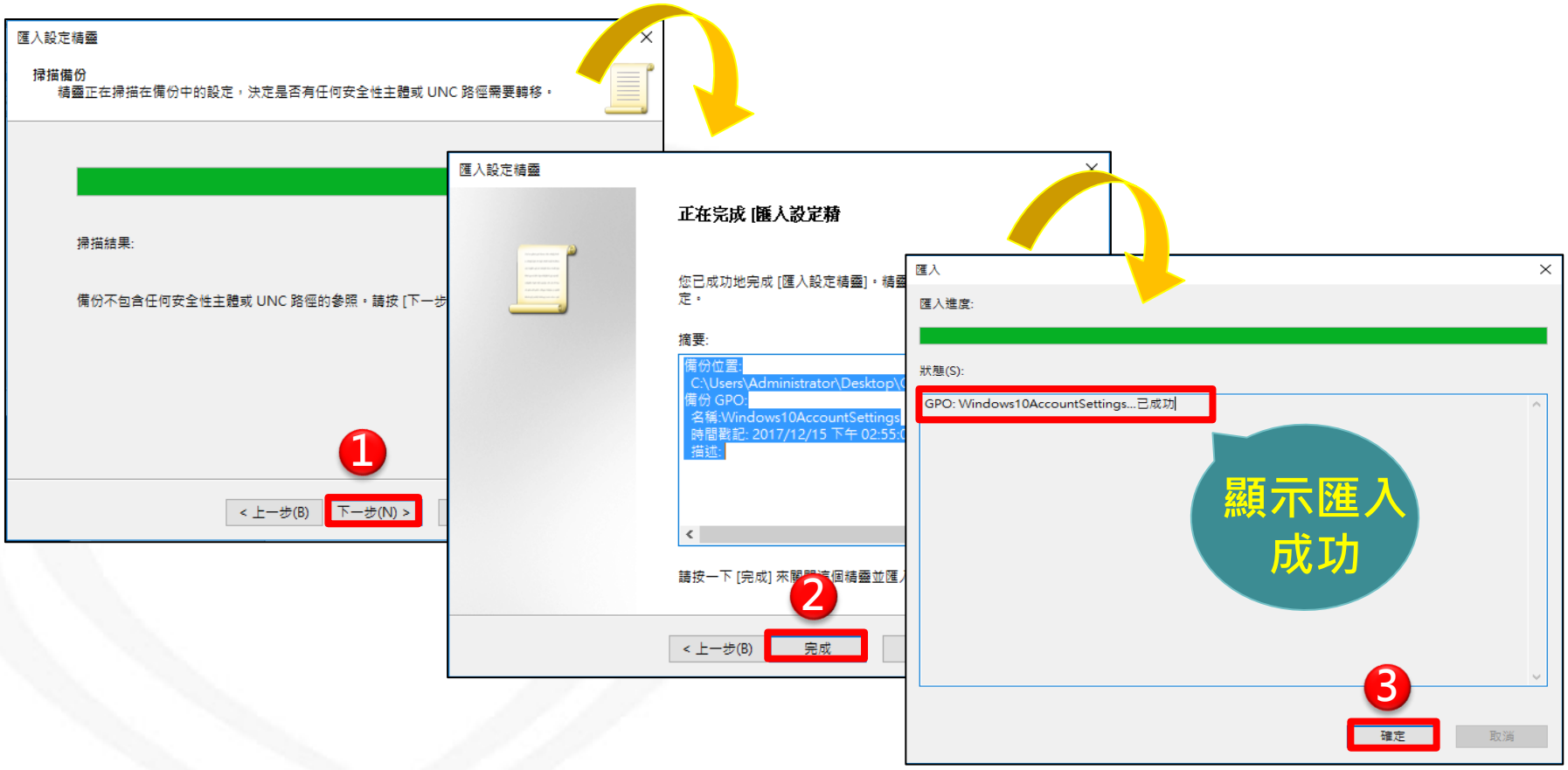
AD環境下調整與測試GCB(4/11)

- 匯入測試的GPO
  - –透過【匯入設定精靈】完成Windows 10之GPO匯入



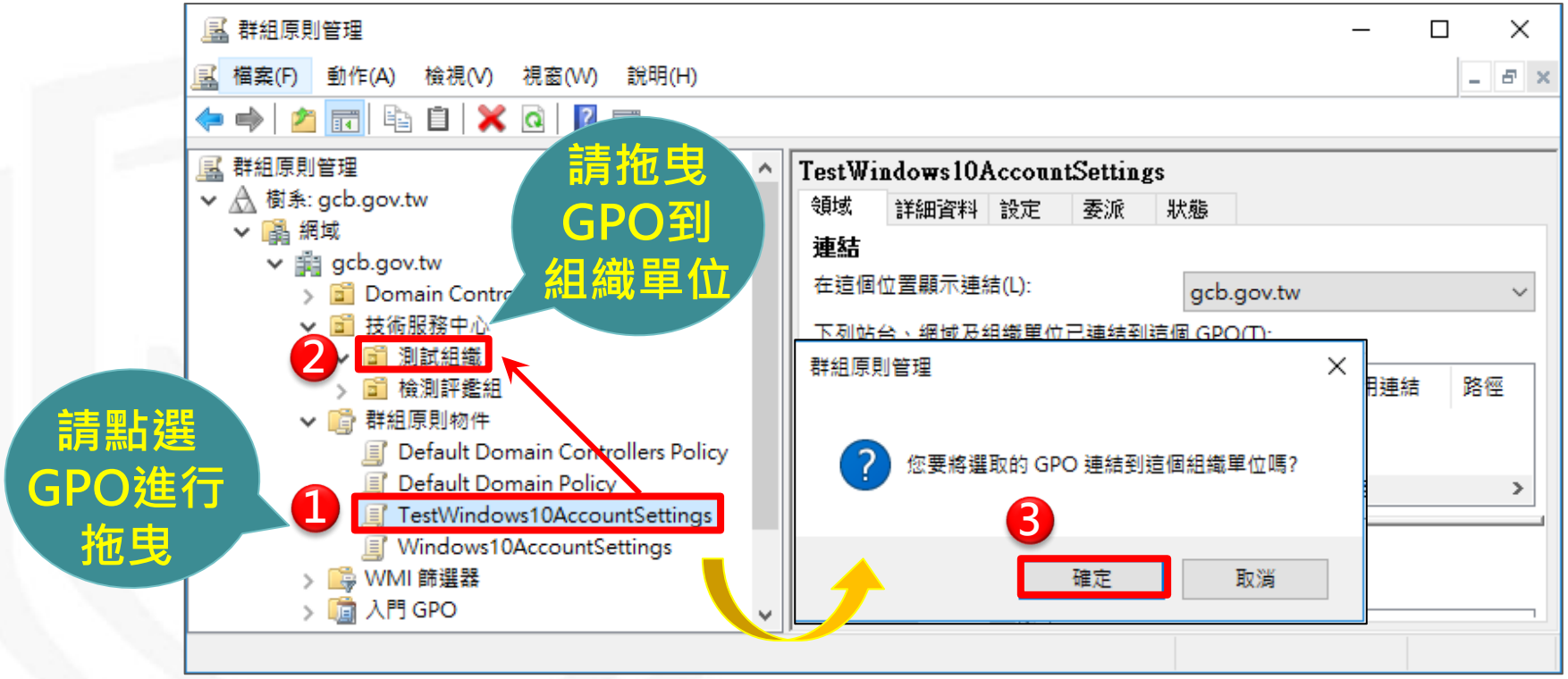
AD環境下調整與測試GCB(5/11)

- 匯入測試的GPO(續)
  - 透過【匯入設定精靈】完成Windows 10之GPO匯入



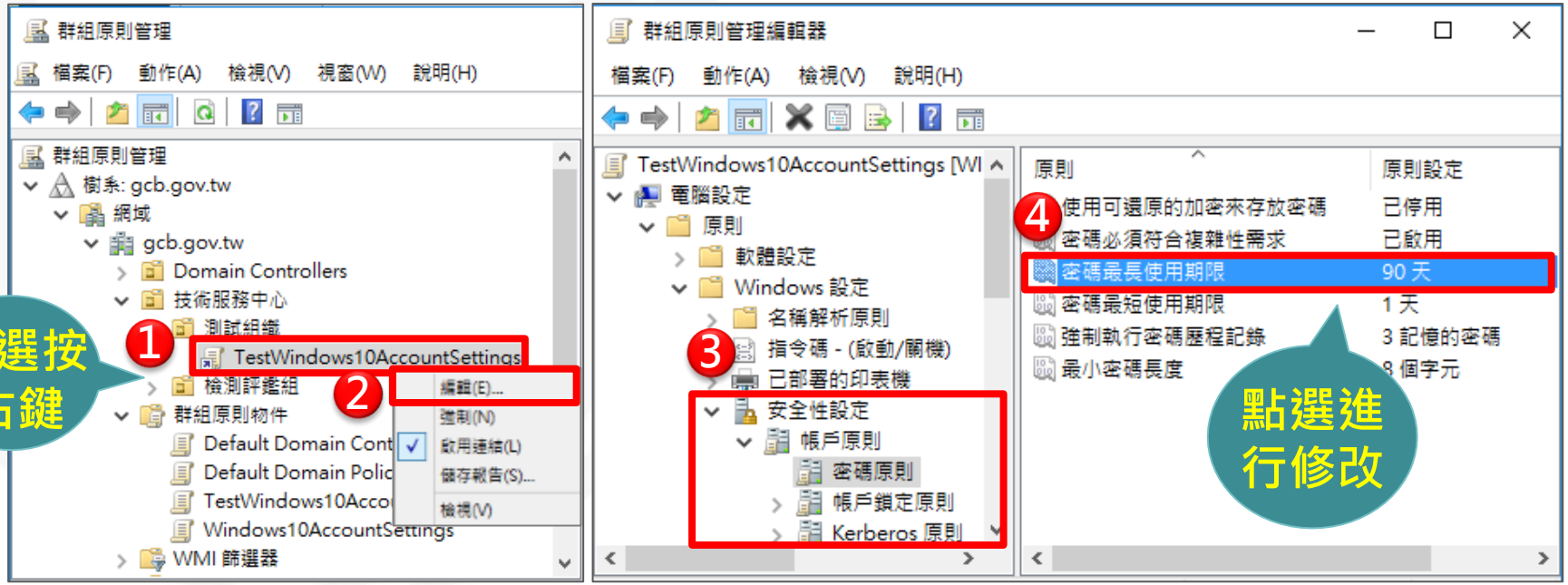
AD環境下調整與測試GCB(6/11)

- 將已匯入GPO的群組原則物件拖曳至組織單位(OU)，完成部署作業



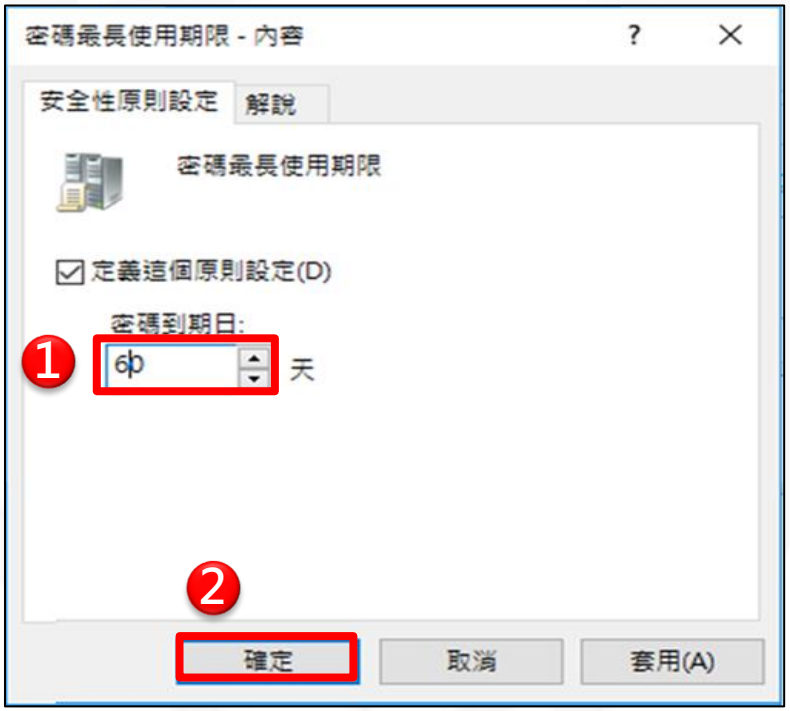
AD環境下調整與測試GCB(7/11)

- 在測試群組原則物件節點按滑鼠右鍵→選擇「編輯」
- 調整組態之設定值
  - 開啟「群組原則管理編輯器」→點選「電腦設定」→點選「原則」→點選「系統管理範本」→點選「TestWin10AccountSettings」，選擇組態進行調整



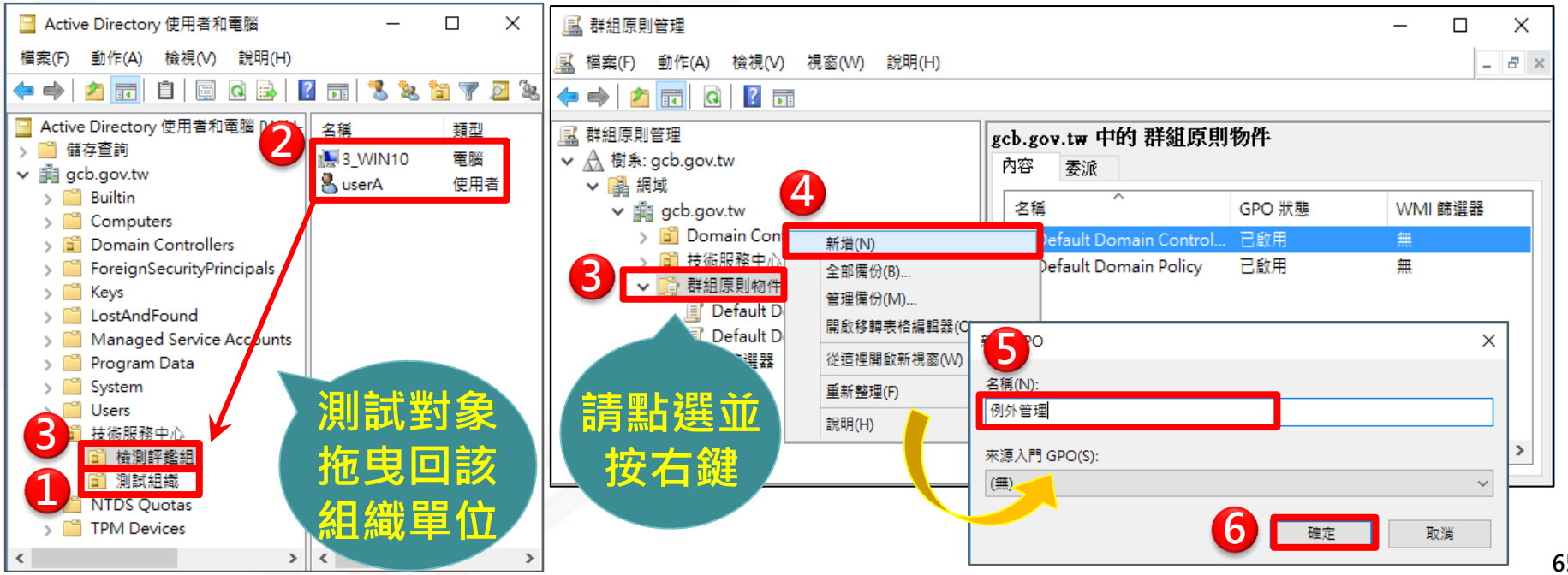
AD環境下調整與測試GCB(8/11)

- 調整組態之設定值
- 在使用者電腦上輸入gpupdate /force更新群組原則
- 測試新設定值是否可排除障礙



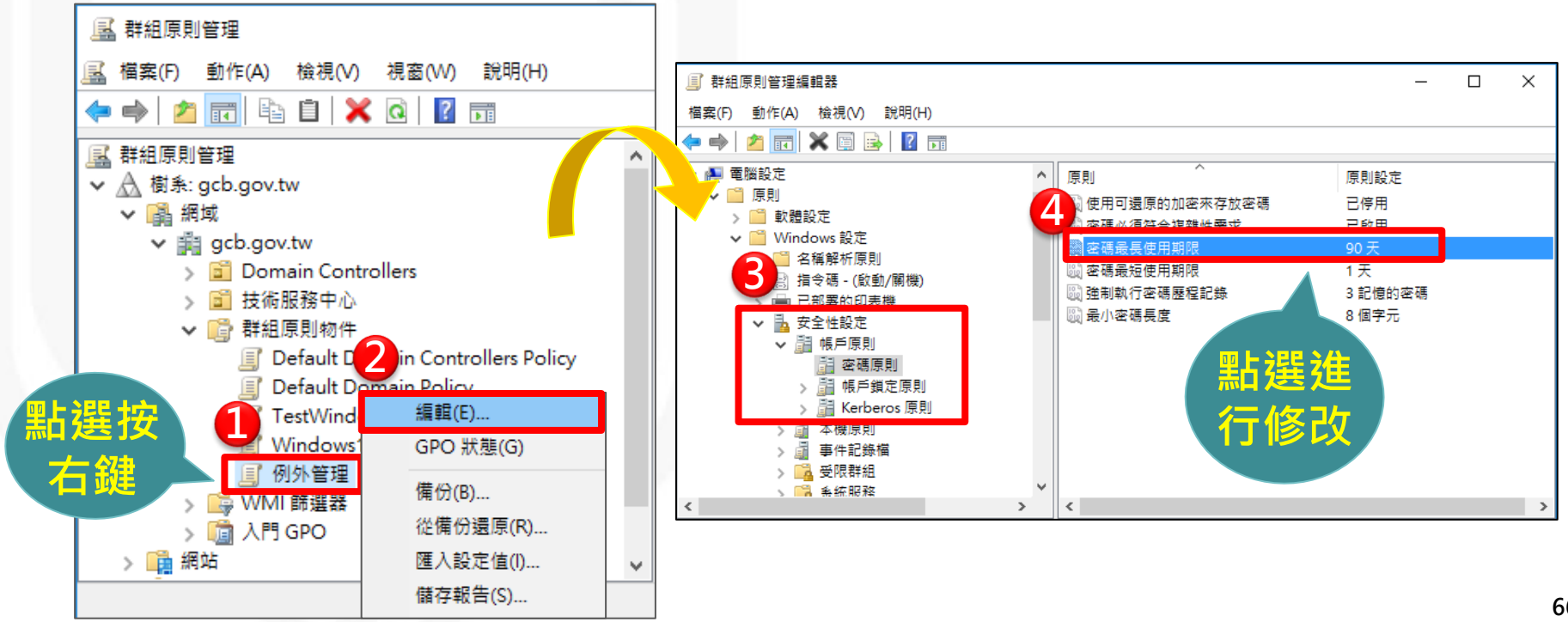
AD環境下調整與測試GCB(9/11)

- 測試完成後
  - –將測試之使用者電腦與帳號拖曳回其所屬之組織單位(OU)
  - –重新建立例外管理GPO
    - ➢在群組原則物件節點按滑鼠右鍵→選擇「新增」
    - ➢在「名稱」欄位→輸入例外管理群組原則物件名稱



AD環境下調整與測試GCB(10/11)

- 測試完成後
  - –在例外管理群組原則物件節點按滑鼠右鍵→選擇「編輯」
    - ➢開啟「群組原則管理編輯器」→點選「電腦設定」→點選「Windows設定」→點選「安全性設定」→點選「密碼原則」，選擇組態進行調整



AD環境下調整與測試GCB(11/11)

- 測試完成後
  - –將例外管理之群組原則物件連結至組織單位(OU)
  - –點選組織單位(OU)，將例外管理的連結順序調整至第一順位

單機環境下調整與測試GCB

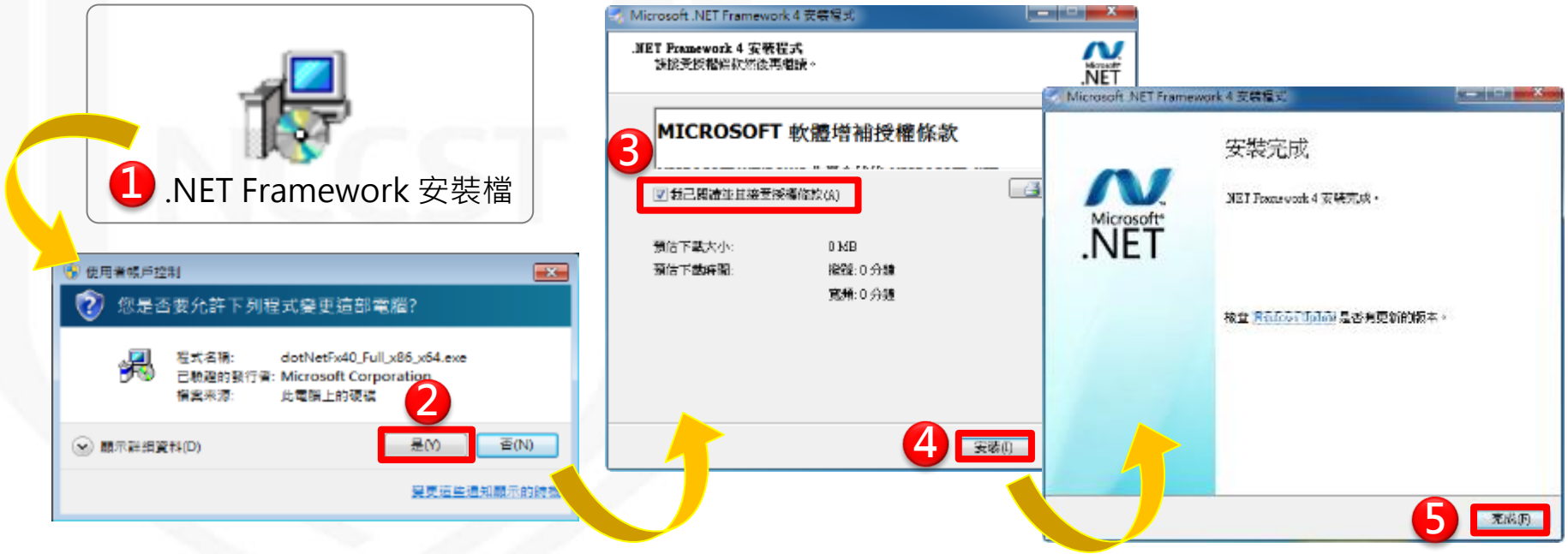
Microsoft Security Compliance Manager (SCM)介紹

- SCM是一免費公用程式，用來建立Windows用戶端與伺服器環境的基準安全性設定
- 適用於：Windows 7、8.1、10
- 下載網址：
  - 需先安裝Microsoft .NET Framework 4
    - https://www.microsoft.com/zh-tw/download/details.aspx?id=17718

  - SCM 4.0
    - https://www.microsoft.com/en-us/download/details.aspx?id=53353

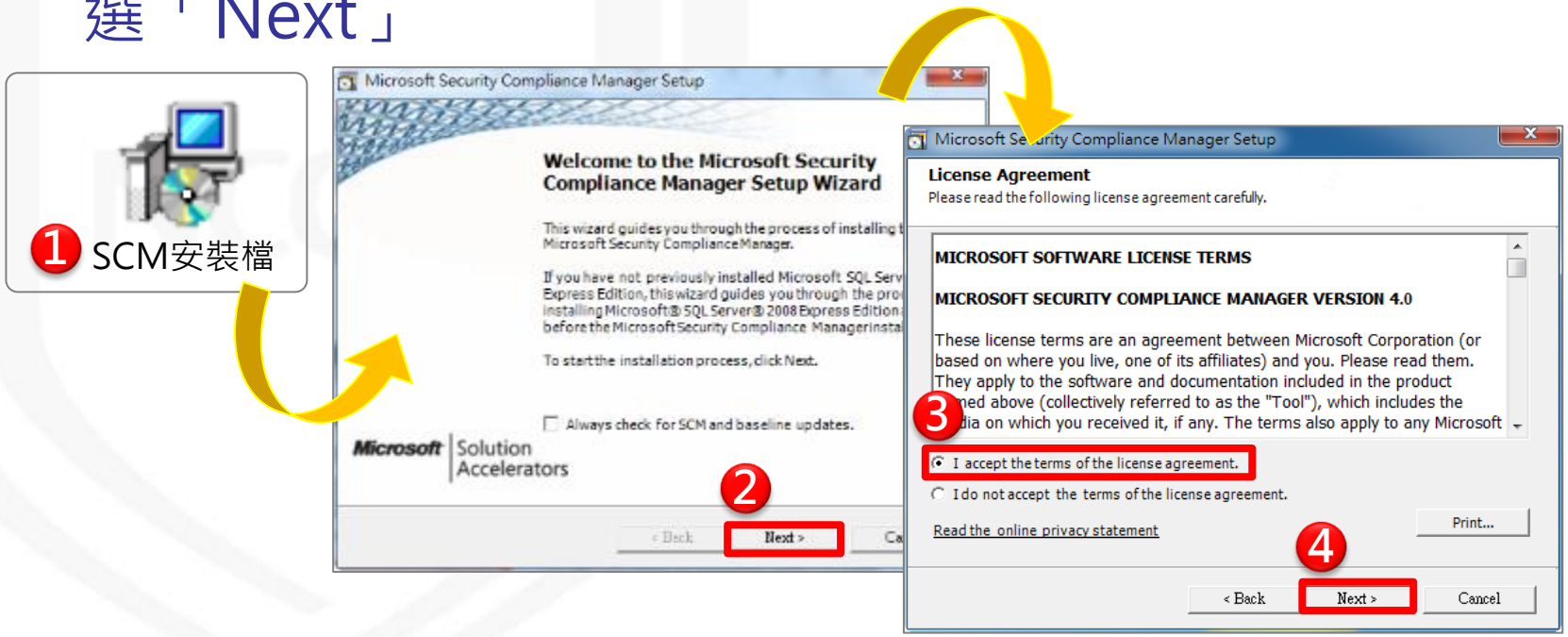
安裝Microsoft .NET Framework

- 執行「Microsoft .NET Framework」安裝檔→點選「是」允許安裝
- 在Microsoft軟體增補授權條款頁面→勾選「我已閱讀並接受授權條款→點選「安裝」→完成



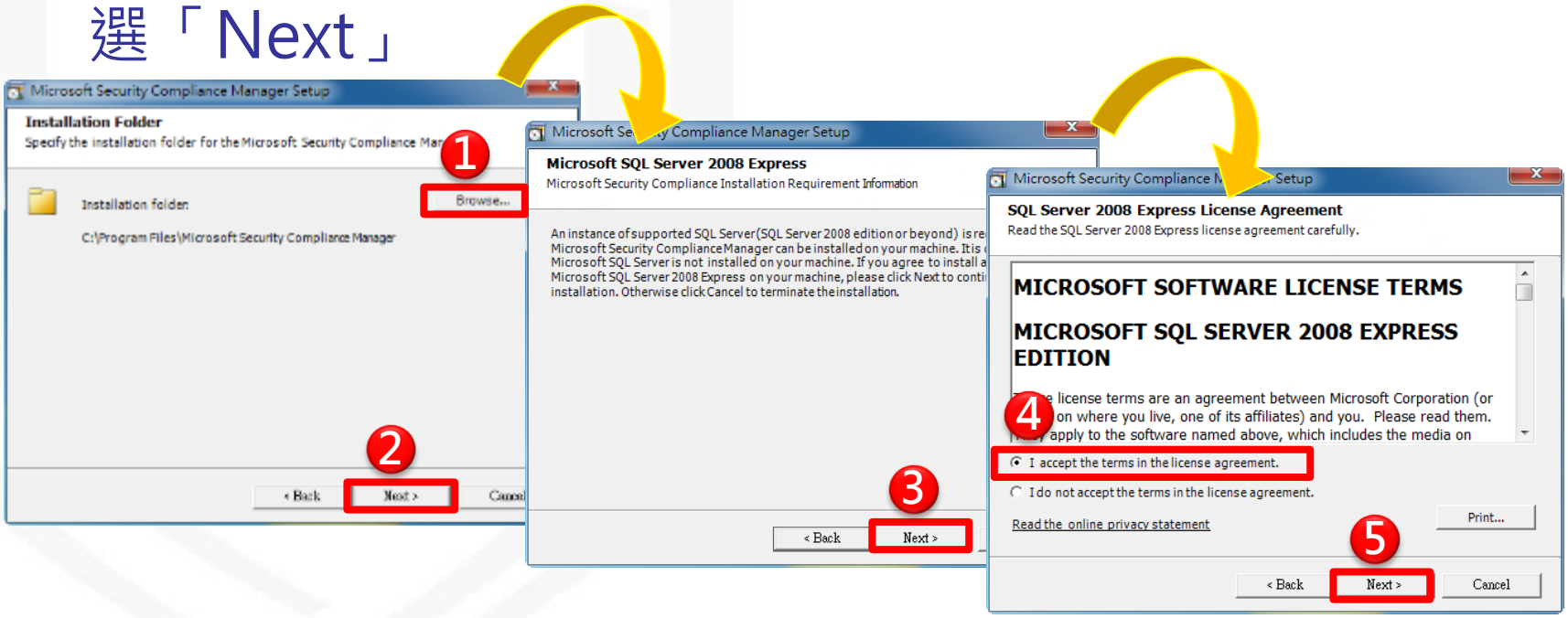
安裝SCM(1/3)

- 執行「SCM 」安裝檔→點選「是」允許安裝
- 在Welcome to the Security Compliance Manager Setup頁面→點選「Next」
- 在License Agreement頁面→勾選接受授權協議→點選「Next」



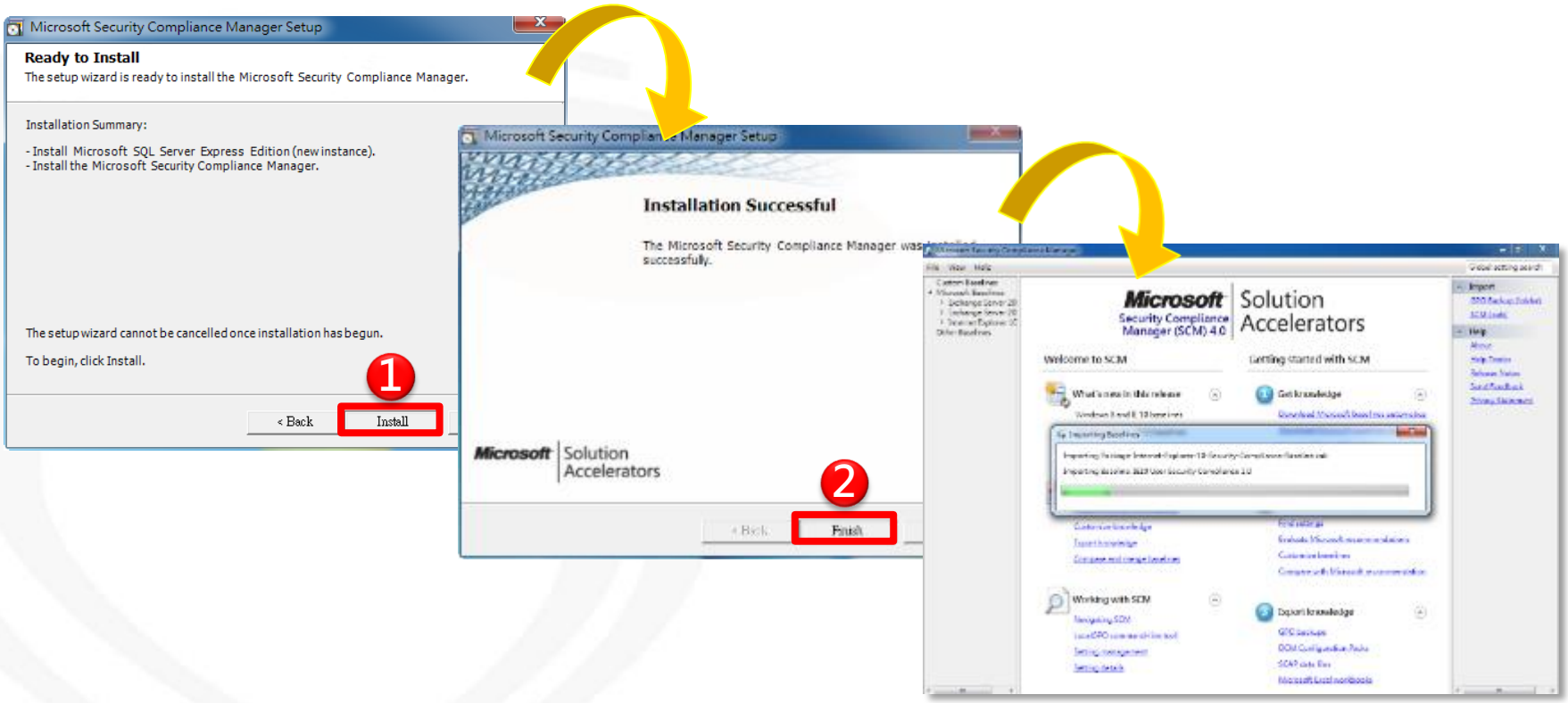
安裝SCM(2/3)

- 在Installation Folder頁面→確認安裝路徑→點選「Next」
- 開始安裝SQL Server 2008 Express→點選「Next」
- 在License Agreement頁面→勾選接受授權協議→點選「Next」



安裝SCM(3/3)

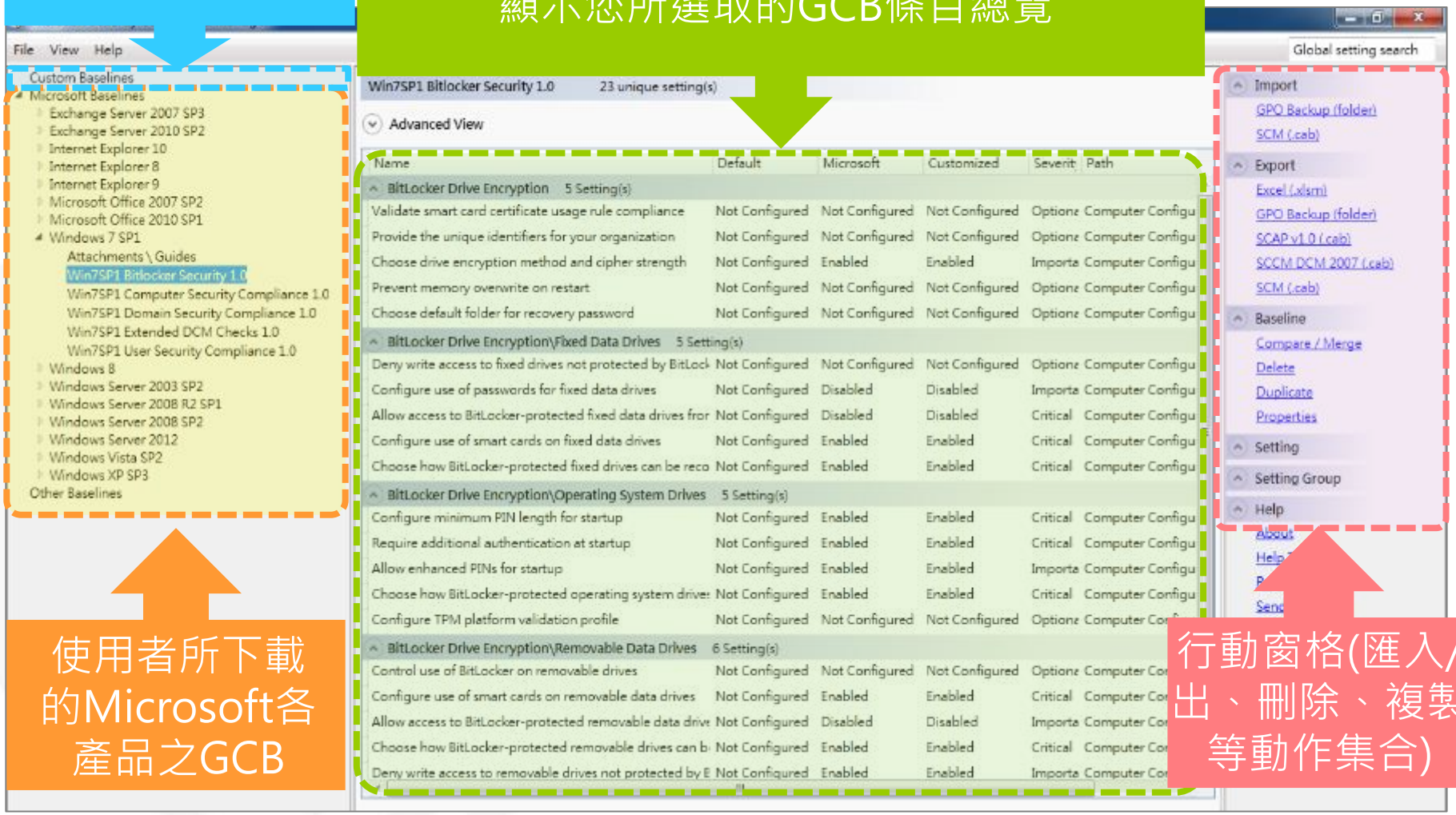
- 在Read to Install頁面→點選「Install」安裝SCM
- 在Installation Successful頁面→點選「Finish」



SCM畫面說明

客製化GCB

顯示您所選取的GCB條目總覽

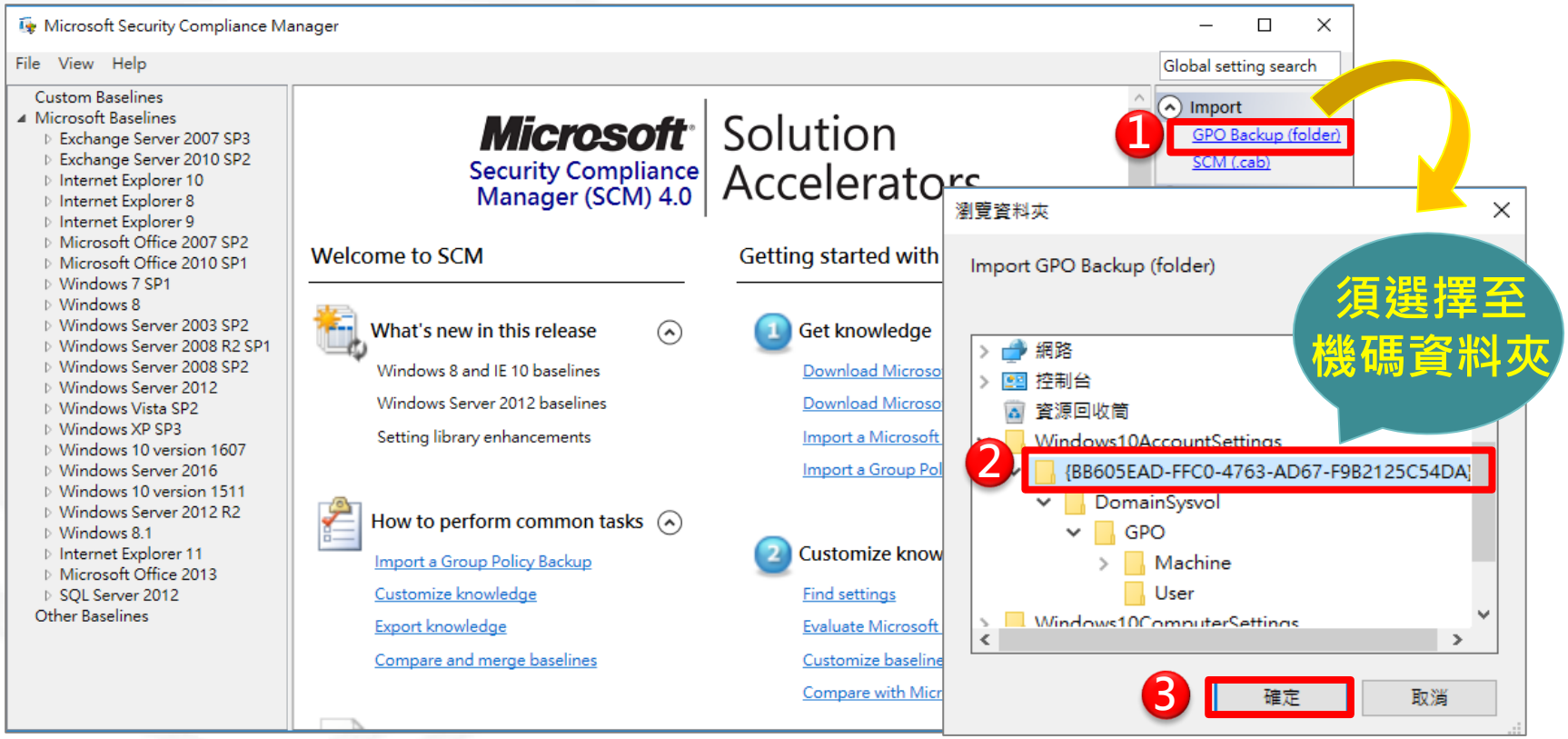


使用者所下載的Microsoft各產品之GCB

行動窗格(匯入/出、刪除、複製等動作集合)

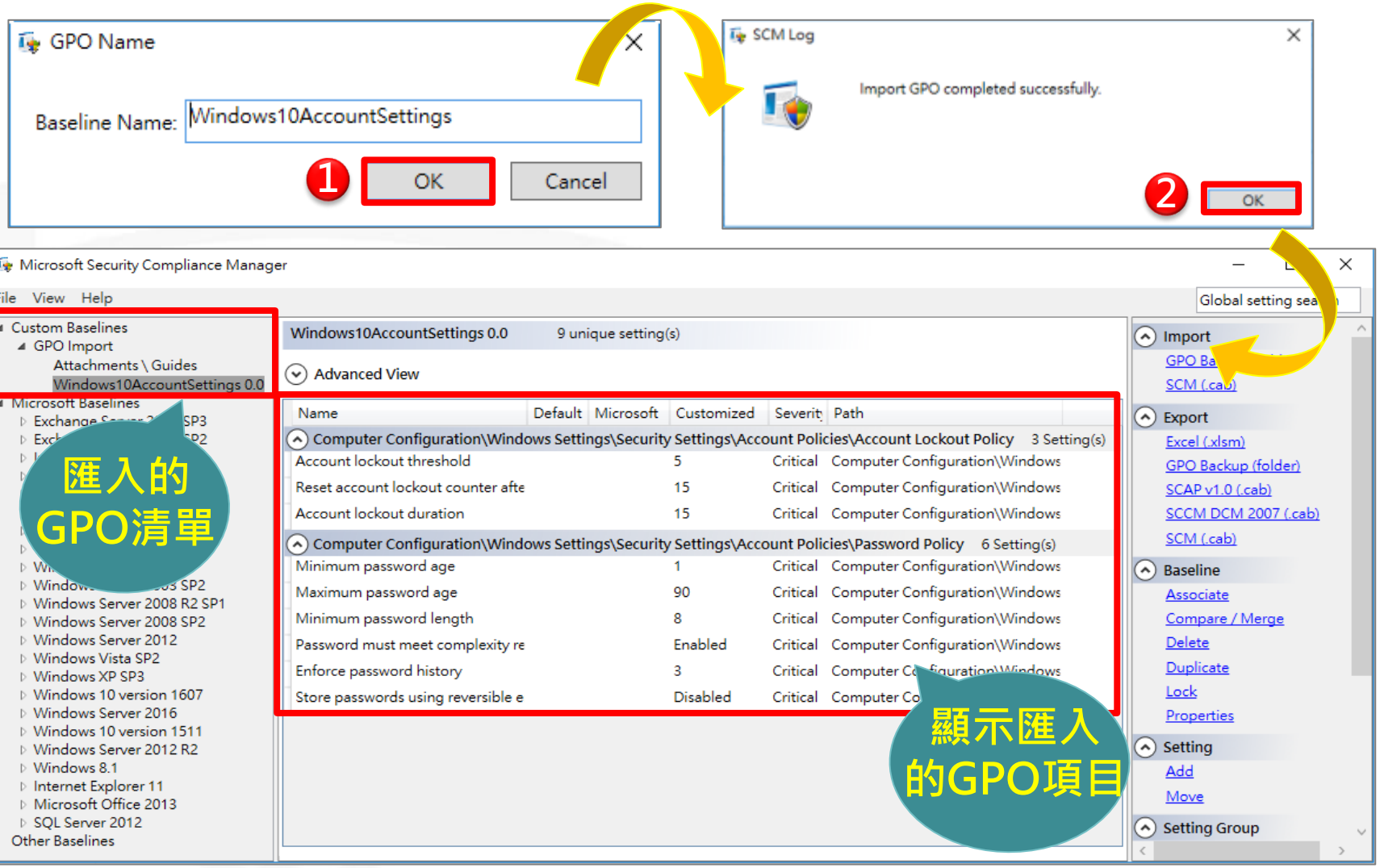
SCM功能介紹-匯入GPO檔(1/2)

- 在行動窗格中選擇Import →點選「GPO Backup (folder) 」
- 選擇欲匯入的GPO目錄下之機碼資料夾→點選「確定」



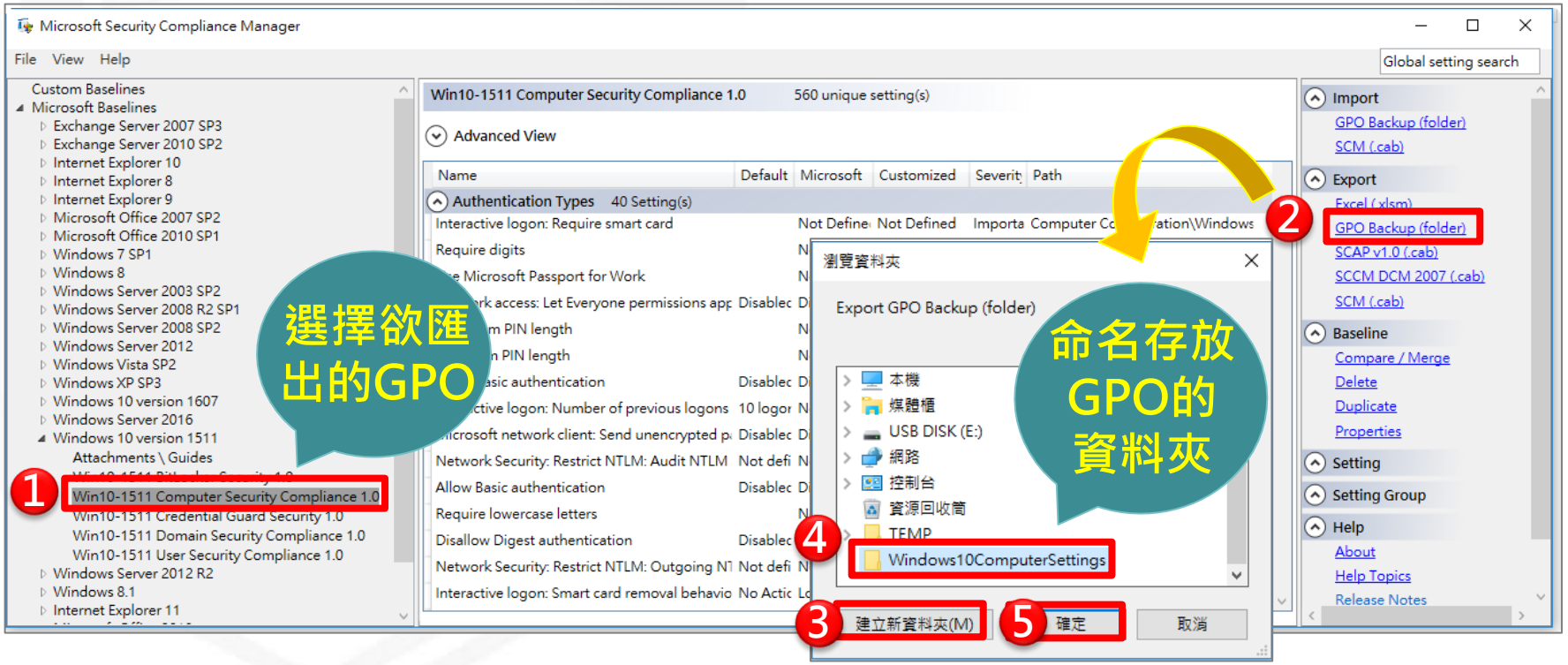
SCM功能介紹-匯入GPO檔(2/2)

- SCM自動帶出GPO名稱→點選「OK」→完成匯入



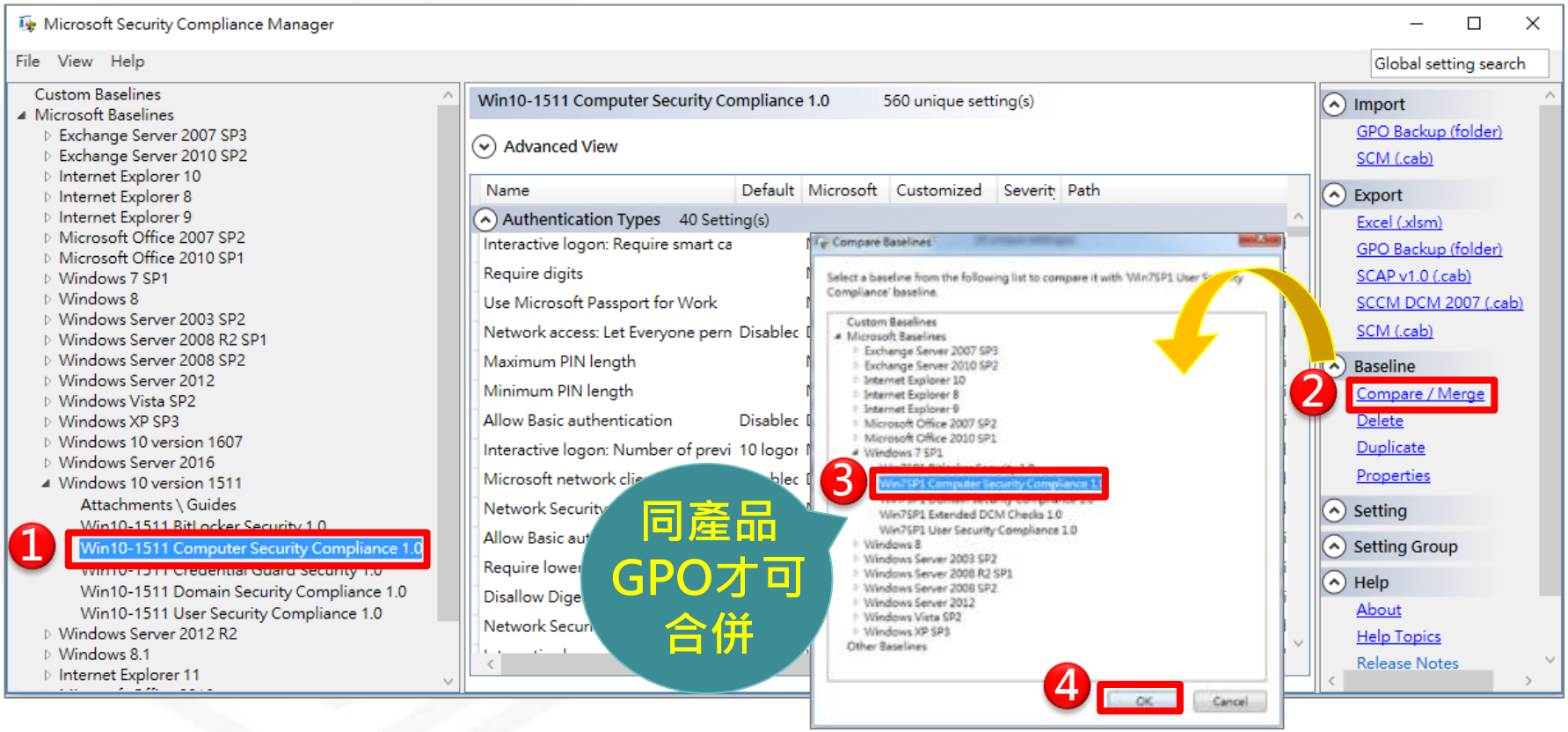
SCM功能介紹-匯出GPO檔

- 在SCM中→點選欲匯出的GPO
- 在行動窗格中選擇Export →點選「GPO Backup folder」→點選「建立新資料夾」→輸入資料夾名稱 → 點選「確定」→完成匯出



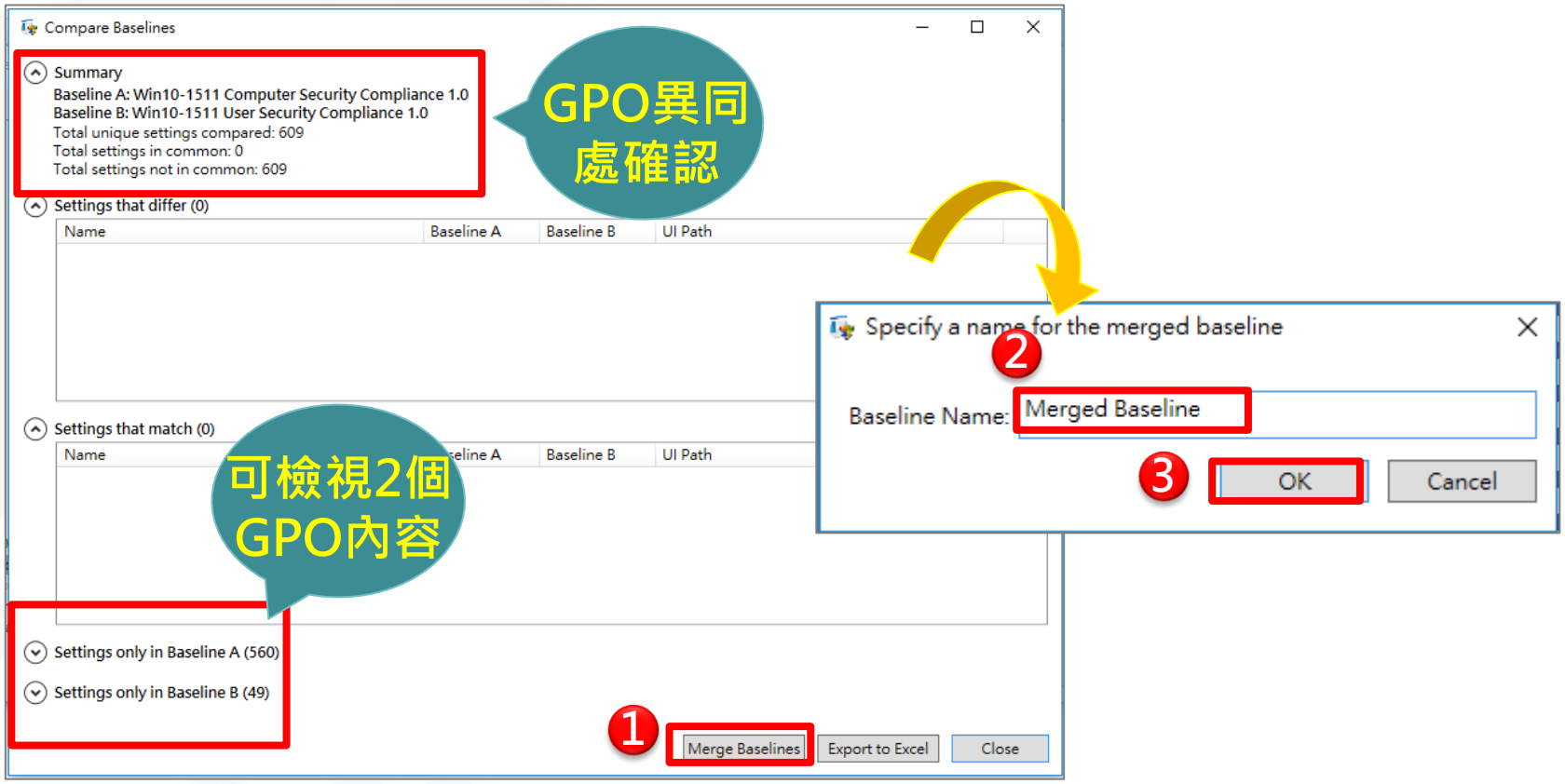
SCM功能介紹-合併GPO檔(1/2)

- 選取第1個GPO檔，在行動窗格中選擇Baseline →點選「Compare/Merge」
- 選取欲合併的GPO檔→點選「OK」



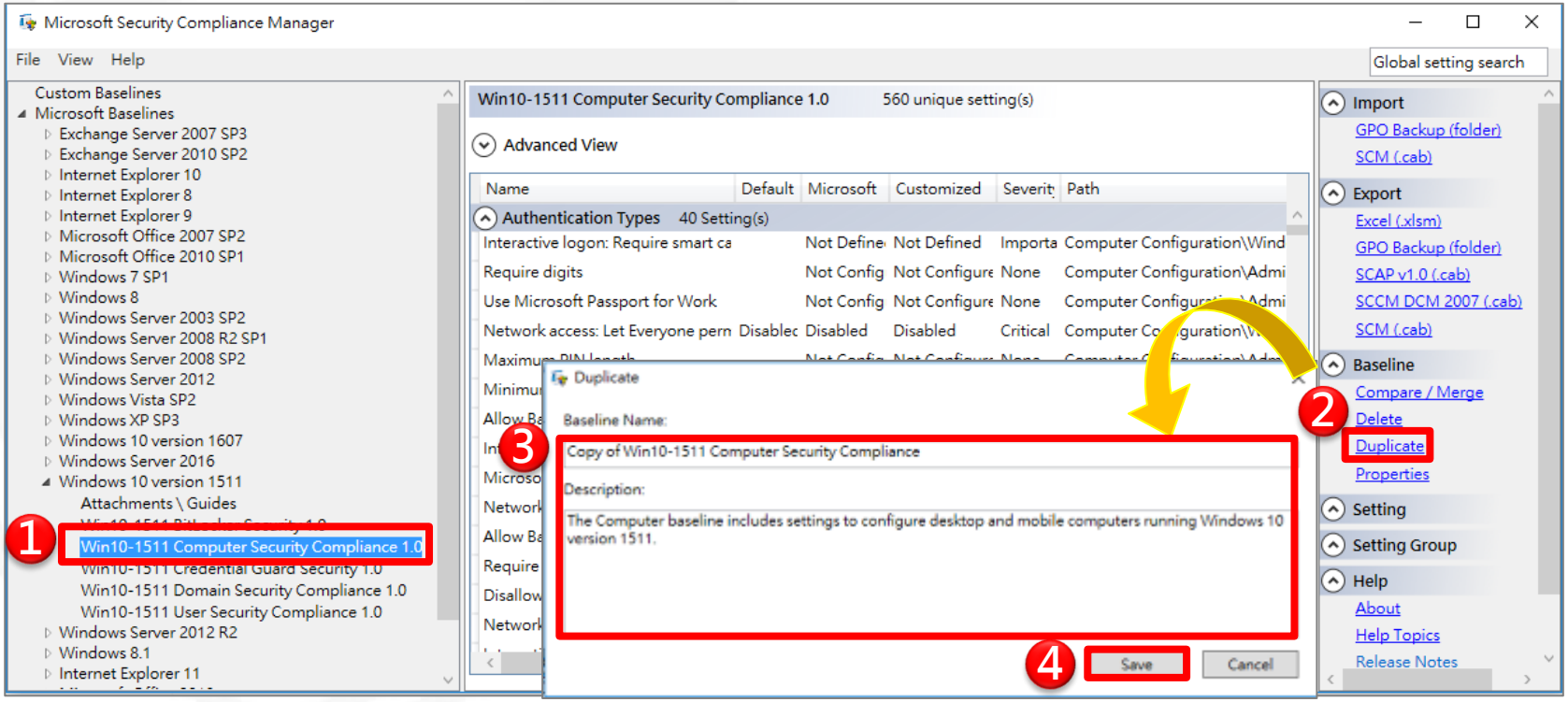
SCM功能介紹-合併GPO檔(2/2)

- 在Compare Baselines視窗中，列出2個GPO異同之處，確認無誤後→點選「Merge Baselines」
- 填入合併後的GPO名稱→點選「OK」→完成合併



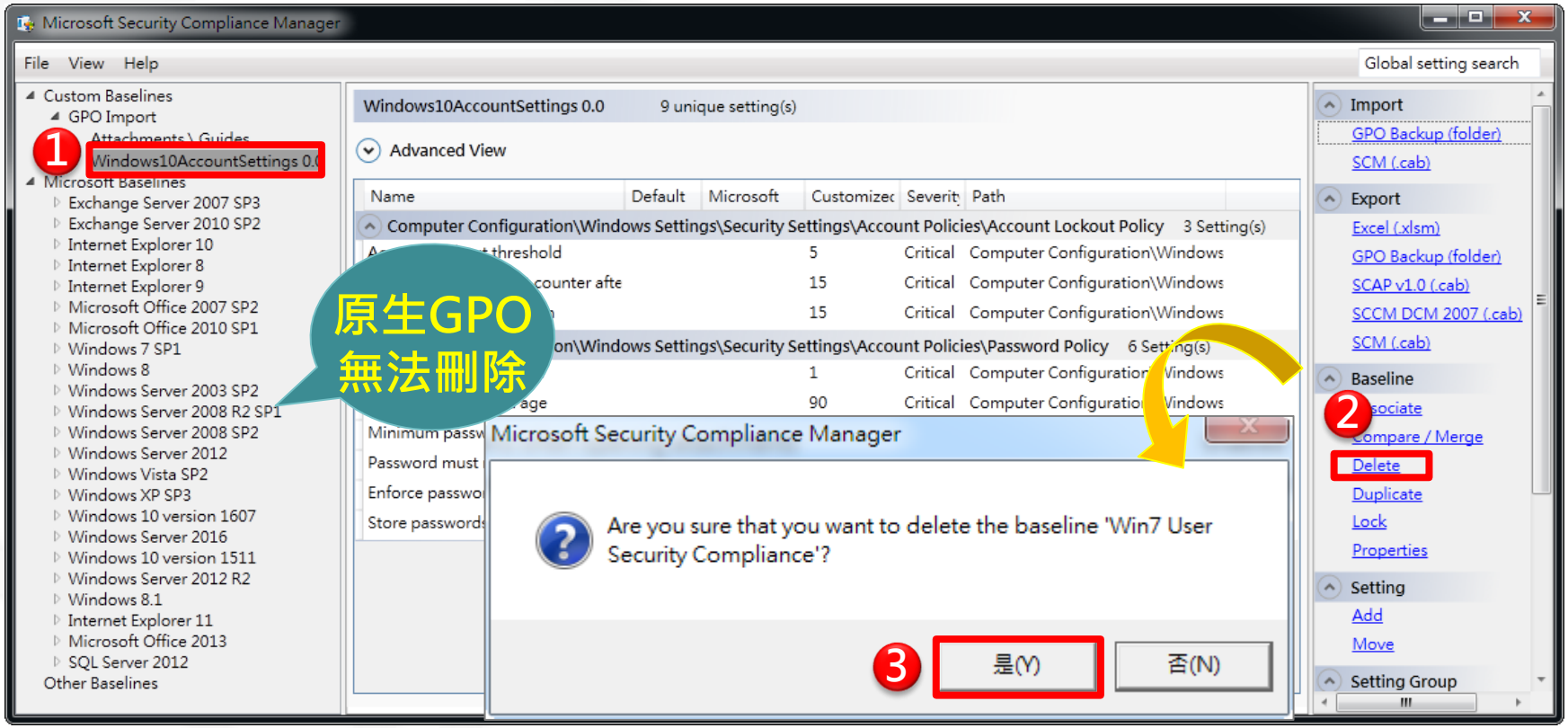
SCM功能介紹-複製GPO檔

- 選取1個SCM原生GPO檔→在行動窗格中選擇Baseline→點選「Duplicate」
- 重新命名GPO檔與修改描述內容→點選「Save」→完成複製



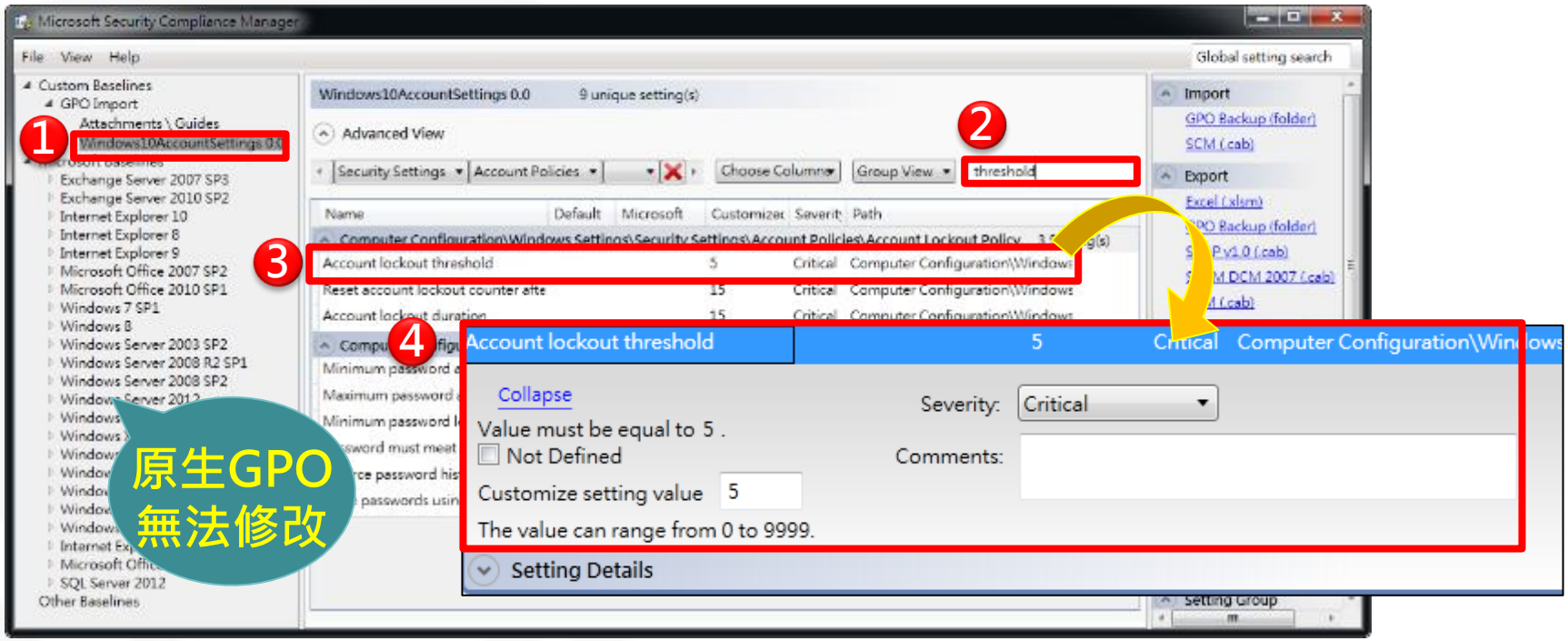
SCM功能介紹-刪除GPO檔

- 選取1個GPO檔→在行動窗格中選擇Baseline→點選「Delete」
- 在確認視窗→點選「是」→完成刪除



SCM功能介紹-修改GPO檔

- 由左視窗選擇GPO檔，並在中間視窗Advanced View以欄位或關鍵字尋找要修改的群組原則
- 點選欲修改的群組原則→調整設定值→完成修改



實作練習-AD部署練習

實作說明

- AD部署環境說明
  - (GCB)Windows Server 2016
    - 帳號：Administrator；密碼：1qaz@WSX3edc
    - 組織單位(OU)：訓練中心
  - (GCB)Windows 10x64_1809 AD
    - 網域帳號：student；密碼：1qaz@WSX3edc
- 請使用AD部署Windows10 GPO，並至Client端
  - 使用Rsop.msc確認部署是否成功
  - 使用Gpresult產製report確認部署是否成功
- VM環境皆已安裝實作練習所需之軟體，並於桌面放置Win10之GPO檔

實作練習-單機部署練習

實作說明

- 單機部署環境說明
  - (GCB)Windows 10x64_1809 Local
    - 本機帳號：Admin ；密碼：1qaz@WSX3edc
- 請使用LocalGPO與LGPO部署Windows10 GPO
  - 使用Gpedit.msc確認部署是否成功
- VM環境皆已安裝實作練習所需之軟體，並於桌面放置Win10之GPO檔

報告完畢
敬請指教