



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

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 shape and "NCCST" text as the logo in the top right corner, but in a light gray color.

NCCST

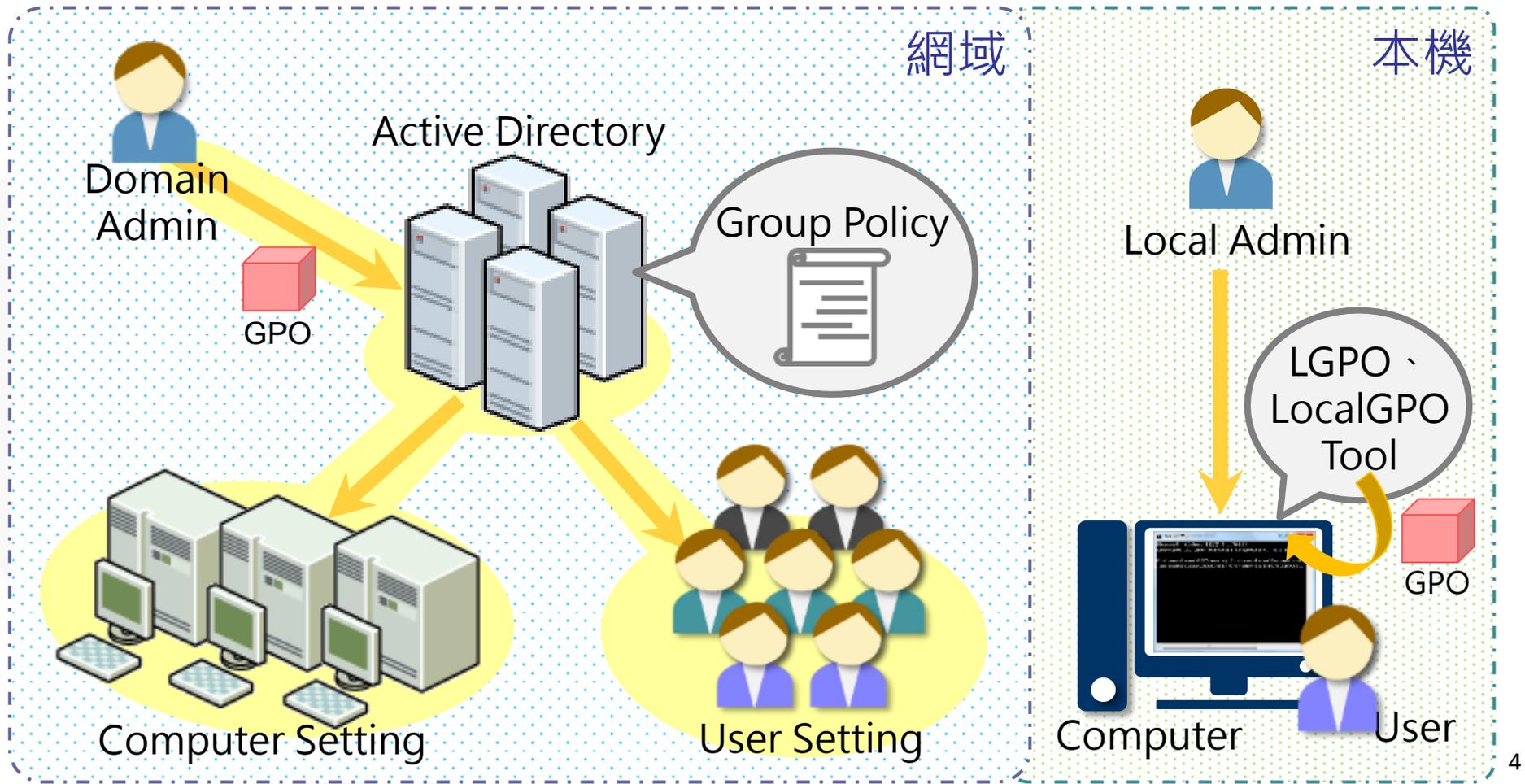
何謂群組原則(1/2)

- 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



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

擔任第一層的身分安全驗證伺服器

2

3

集中維護網域內的共用資源

配置各階層組織單位，給予不同原則限制

4

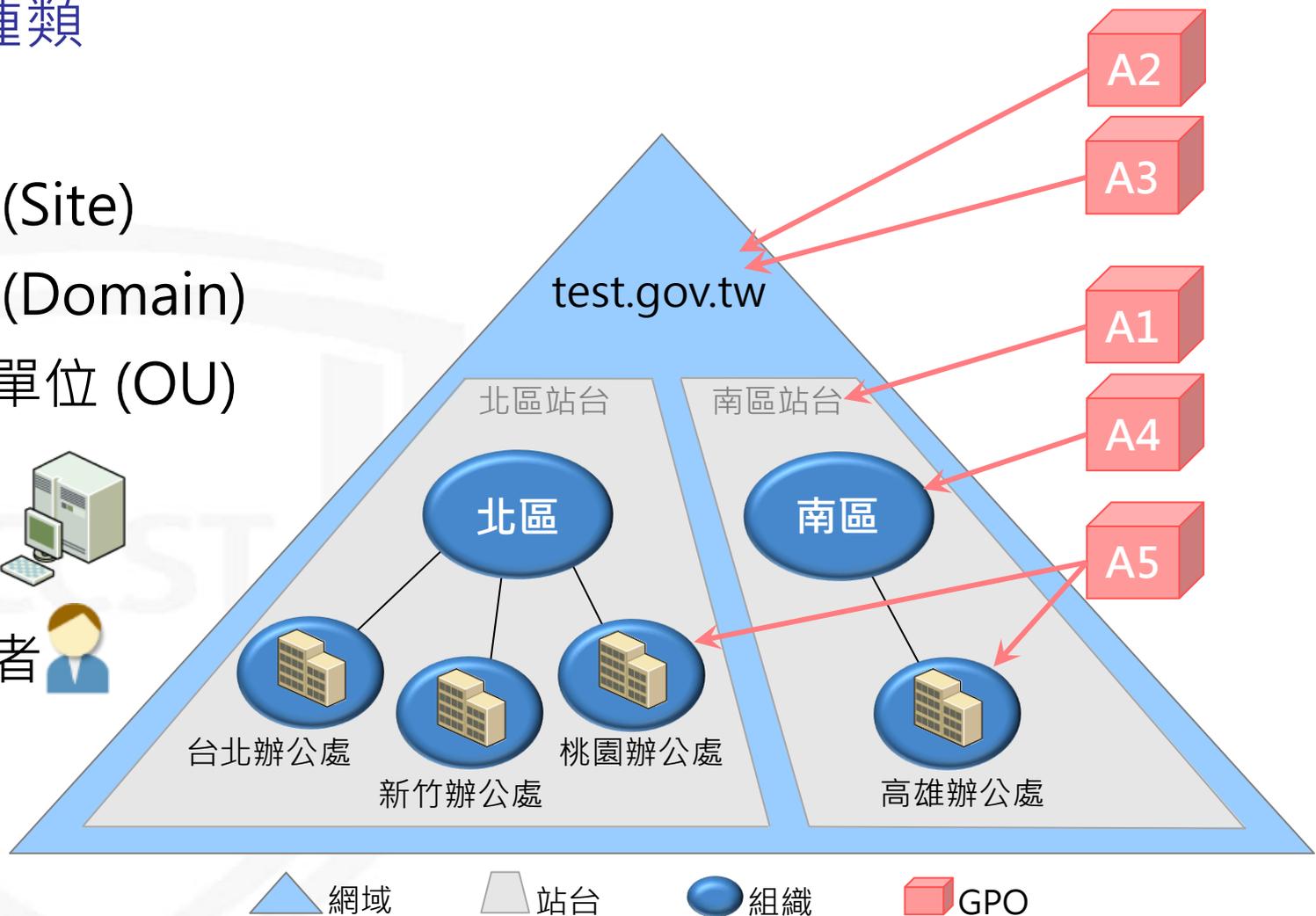
群組原則的關聯對象

- 連結種類

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

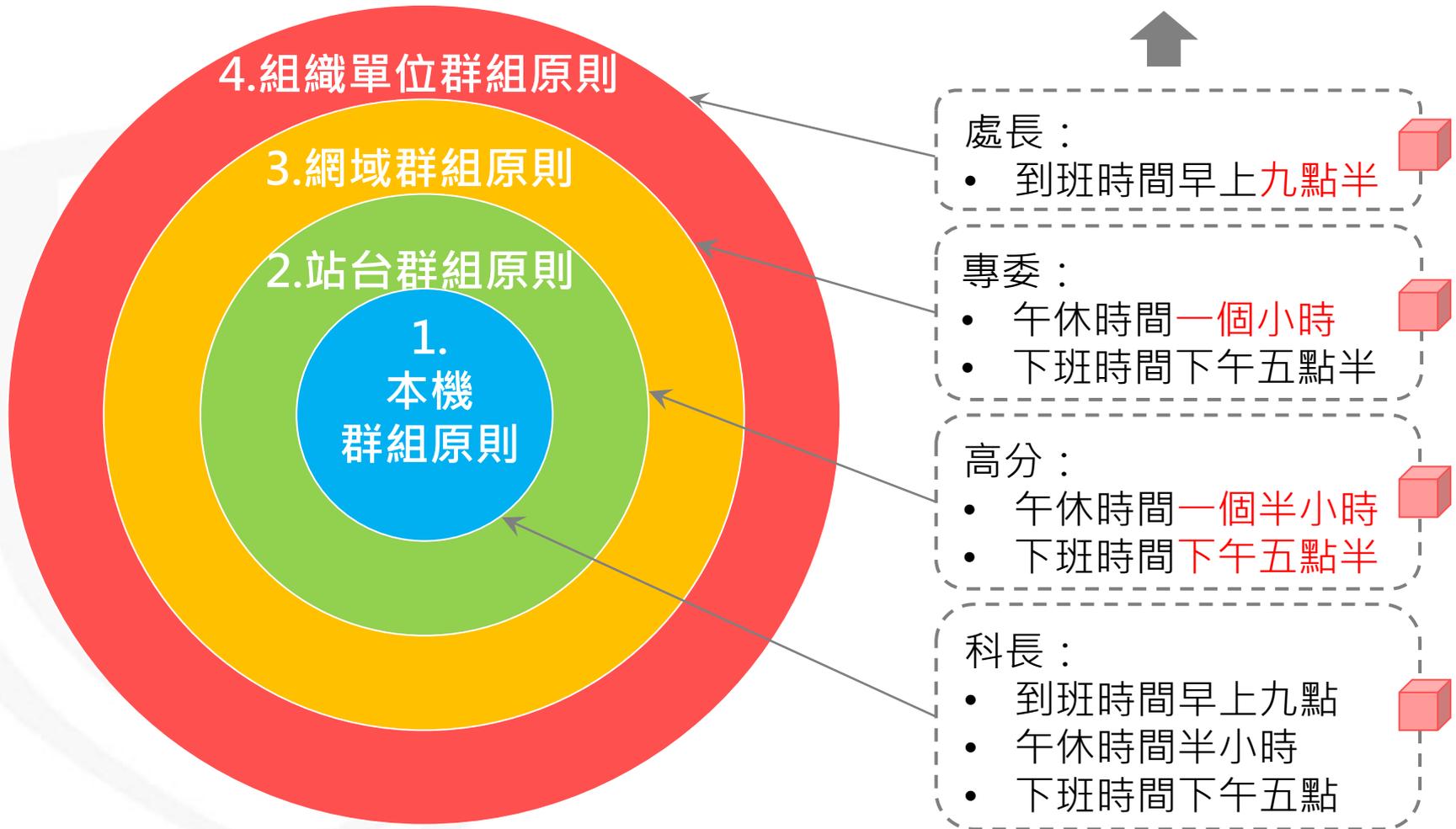
- 對象

- 電腦 
- 使用者 



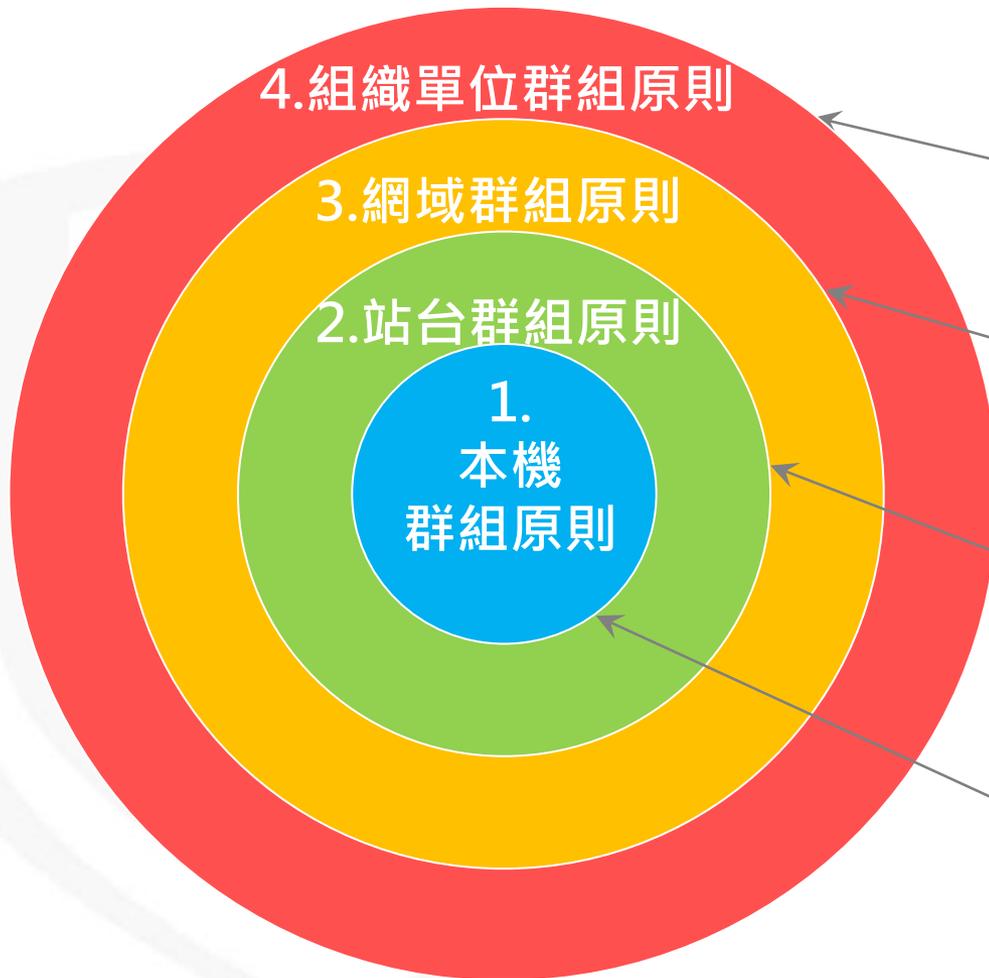
群組原則的套用順序

到班時間=? 午休時間=? 下班時間=?



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

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 Users and Computers console for the domain gcb.gov.tw. The interface is divided into a left-hand navigation pane and a right-hand main pane. The left pane shows a tree view of the domain structure, including folders for Built-in, Computers, Domain Controllers, ForeignSecurityPrincipals, Keys, LostAndFound, Managed Service Accounts, Program Data, System, and Users. Under the Users folder, there are sub-folders for 技術服務中心, 檢測評鑑組, and 測試組織. The right pane displays a table of objects in the selected container. The table has columns for Name (名稱), Type (類型), and Description (描述). The objects listed are 3_WIN10 (Computer) and userA (User). Red boxes highlight the domain name in the left pane, the 3_WIN10 and userA entries in the right pane, and the 技術服務中心 folder and its sub-folders in the left pane. Red arrows point from the 技術服務中心 folder to its sub-folders. Five callout bubbles provide additional context: '網域' (Domain) points to the domain name; '加入網域內的電腦' (Add computers in the domain) points to the 3_WIN10 entry; '加入網域內的使用者' (Add users in the domain) points to the userA entry; '組織單位 (OU)' (Organizational Unit) points to the 技術服務中心 folder; '上層組織單位 (OU)' (Parent Organizational Unit) points to the 技術服務中心 folder; and '下層組織單位 (OU)' (Child Organizational Unit) points to the sub-folders under 技術服務中心.

名稱	類型	描述
3_WIN10	電腦	
userA	使用者	

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)

有獎徵答

NCCST

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

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

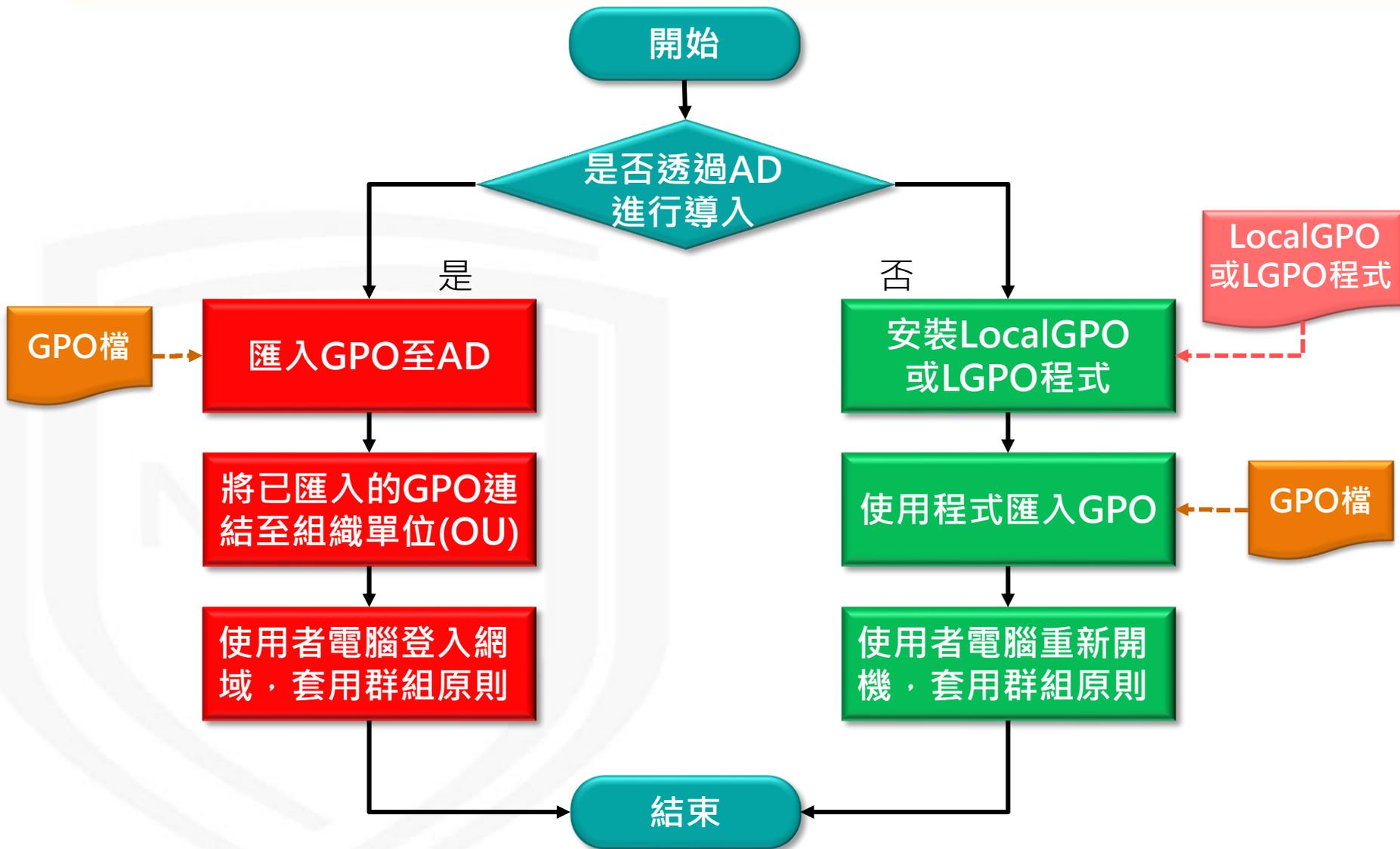
檢測評鑑組：

- 密碼到期3天前提示

GCB導入流程

NCCST

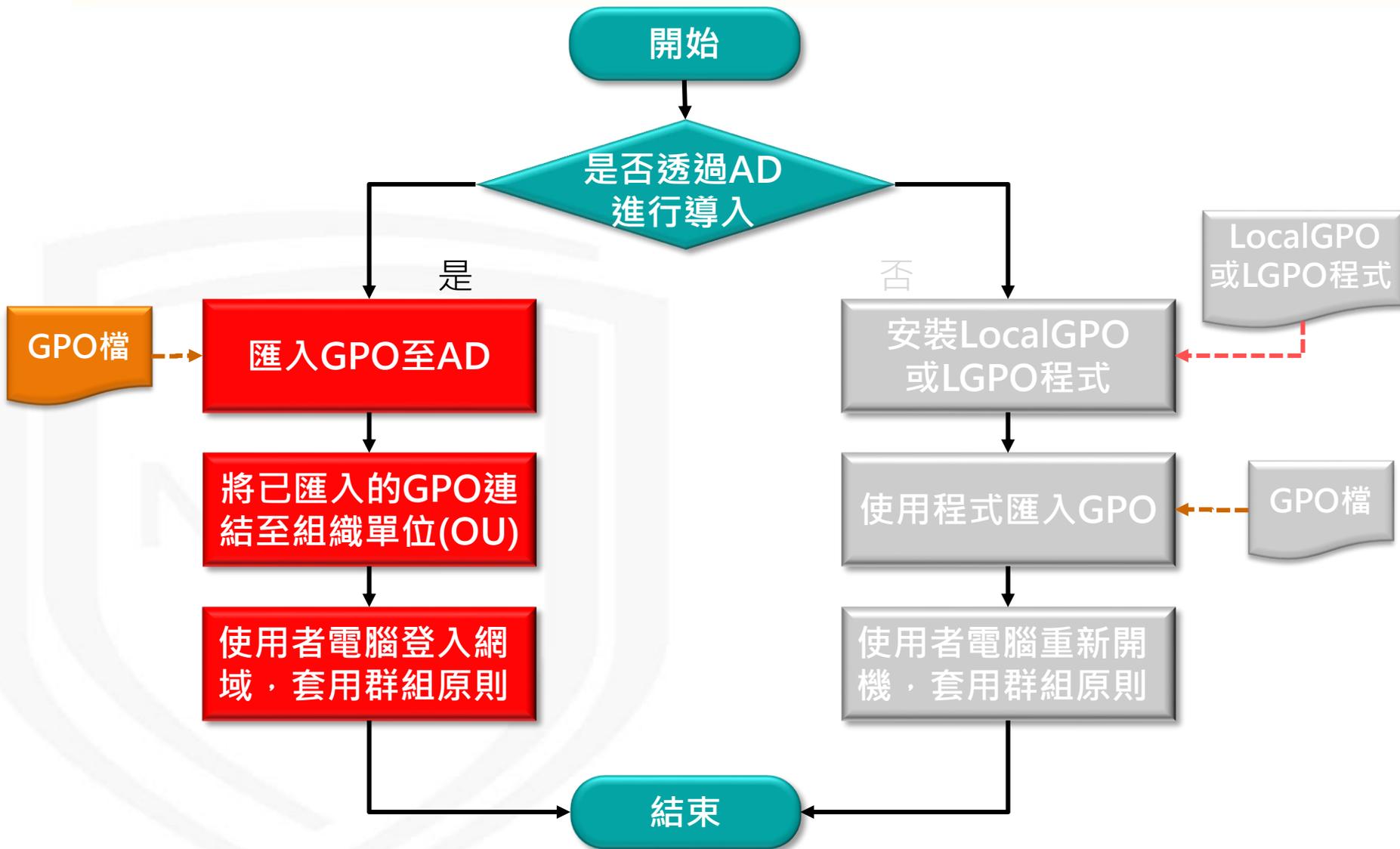
GCB導入流程



使用AD導入GCB

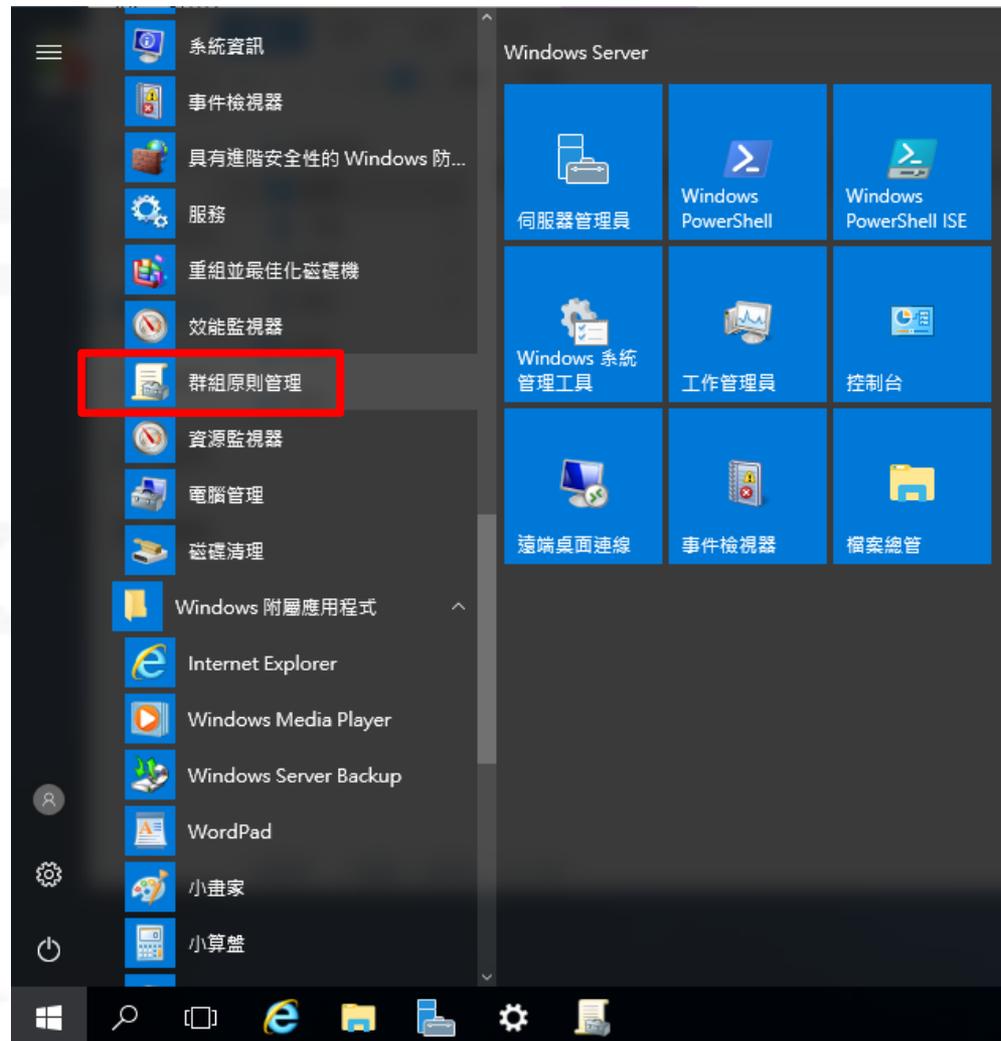
NCCST

GCB導入流程



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



請點選並按右鍵

1 2 3 4

名稱	GPO 狀態	WMI 篩選器
Default Domain Control...	已啟用	無
Default Domain Policy	已啟用	無

新增 GPO

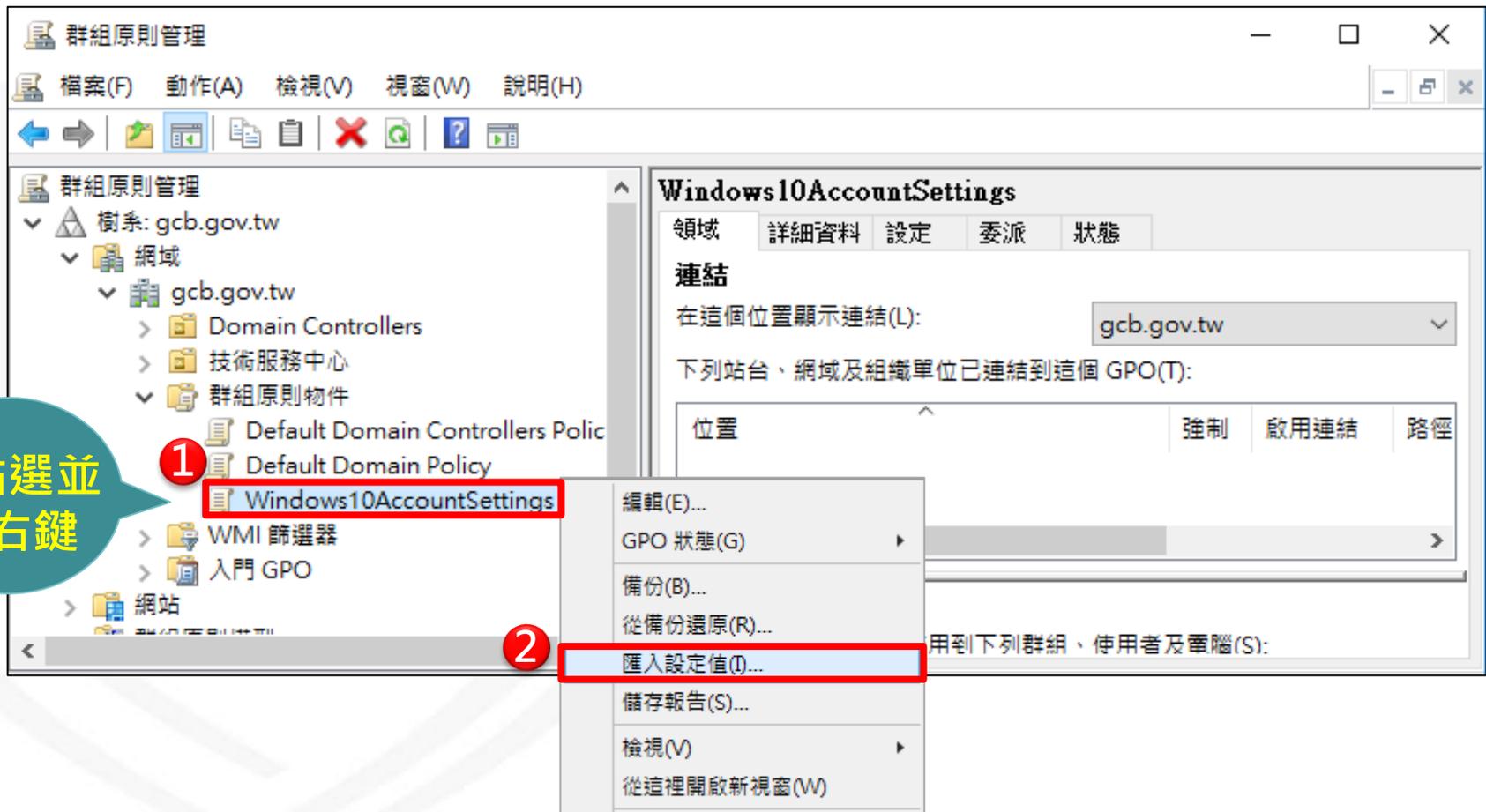
名稱(N): Windows10AccountSettings

來源入門 GPO(S): (無)

確定 取消

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」



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

- 網域
 - gcb.gov.tw
 - Domain Controllers
 - 技術服務中心
 - 群組原則物件
 - Default Domain Controllers Polic
 - Default Domain Policy
 - Windows10AccountSettings**
 - WMI 篩選器
 - 入門 GPO
 - 網站

Windows10AccountSettings

領域 詳細資料 設定 委派 狀態

連結

在這個位置顯示連結(L): gcb.gov.tw

下列站台、網域及組織單位已連結到這個 GPO(T):

位置	強制	啟用連結	路徑
----	----	------	----

用下列群組、使用者及電腦(S):

請點選並按右鍵

1

2

編輯(E)...

GPO 狀態(G)

備份(B)...

從備份還原(R)...

匯入設定值(I)...

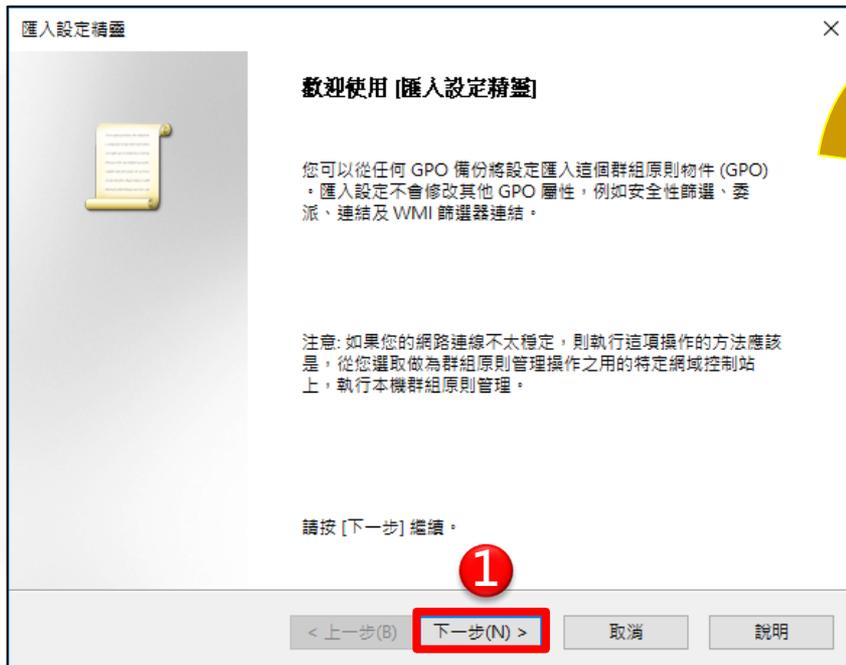
儲存報告(S)...

檢視(V)

從這裡開啟新視窗(W)

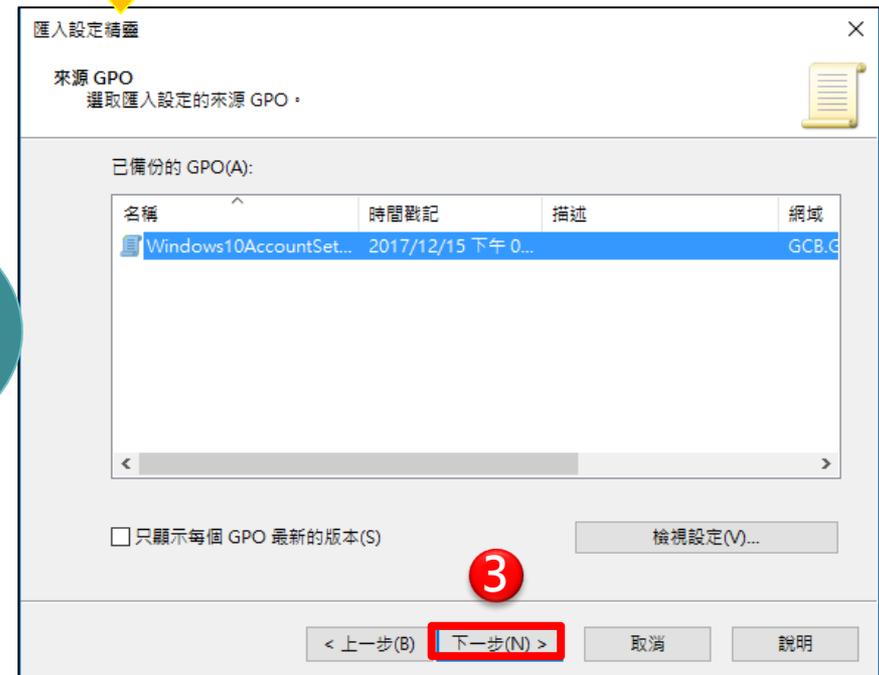
匯入GPO至AD(4/6)

- 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」



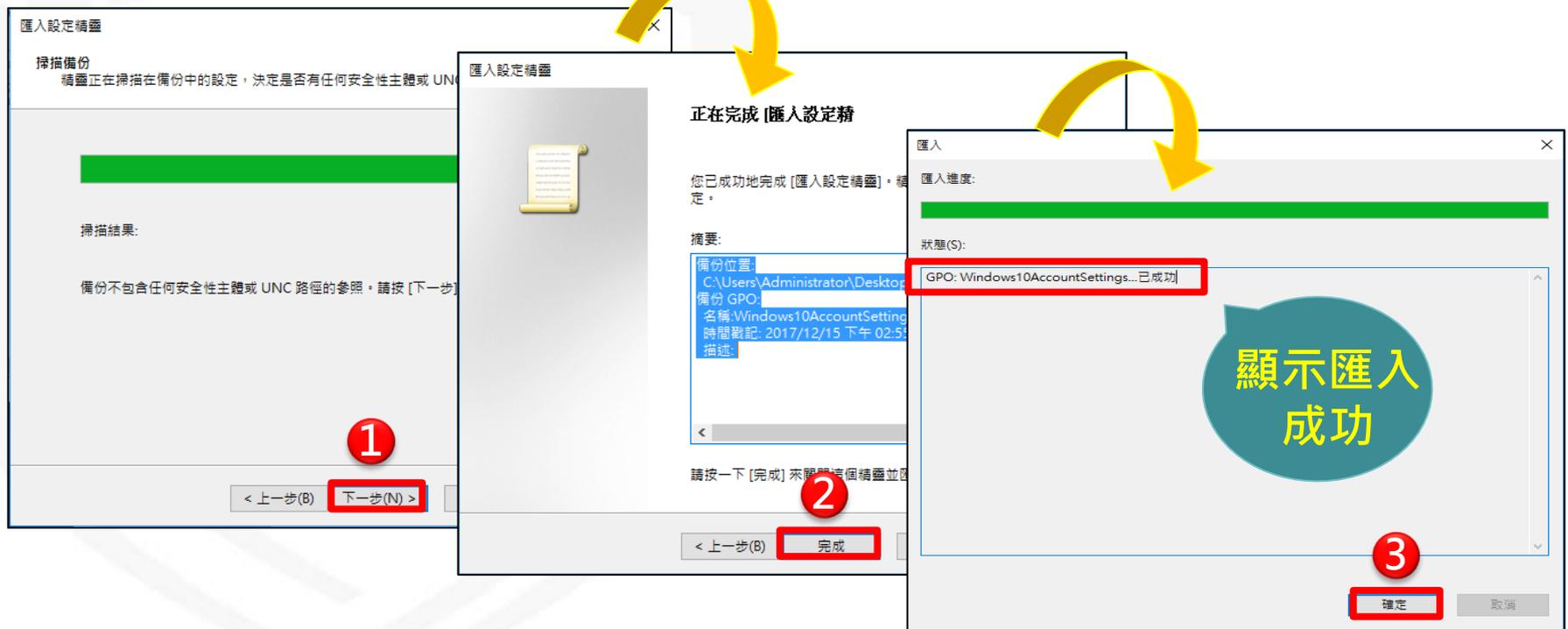
匯入GPO至AD(5/6)

- 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



匯入設定精靈

掃描備份
精靈正在掃描在備份中的設定，決定是否有任何安全性主體或 UNC 路徑的參照。

掃描結果:
備份不包含任何安全性主體或 UNC 路徑的參照，請按 [下一步]

1

< 上一步(B) **下一步(N) >**

匯入設定精靈

正在完成 [匯入設定精靈]

您已成功地完成 [匯入設定精靈]，請按 [完成] 來關閉這個精靈並繼續。

摘要:
備份位置: C:\Users\Administrator\Desktop
備份 GPO: Windows10AccountSettings...
名稱: Windows10AccountSettings...
時間戳記: 2017/12/15 下午 02:55
描述:

2

< 上一步(B) **完成**

匯入

匯入進度:
狀態(S): GPO: Windows10AccountSettings... 已成功]

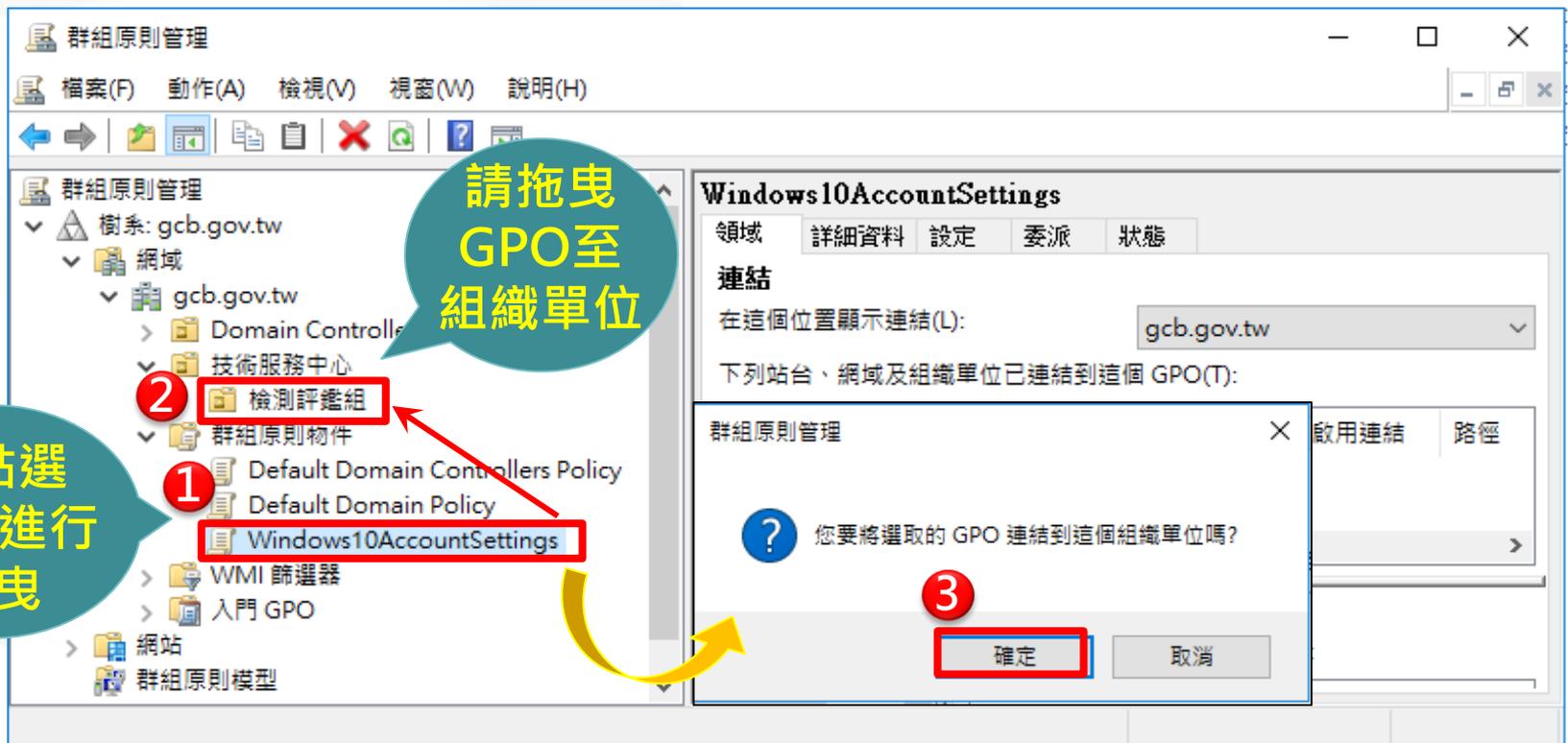
顯示匯入成功

3

確定 取消

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



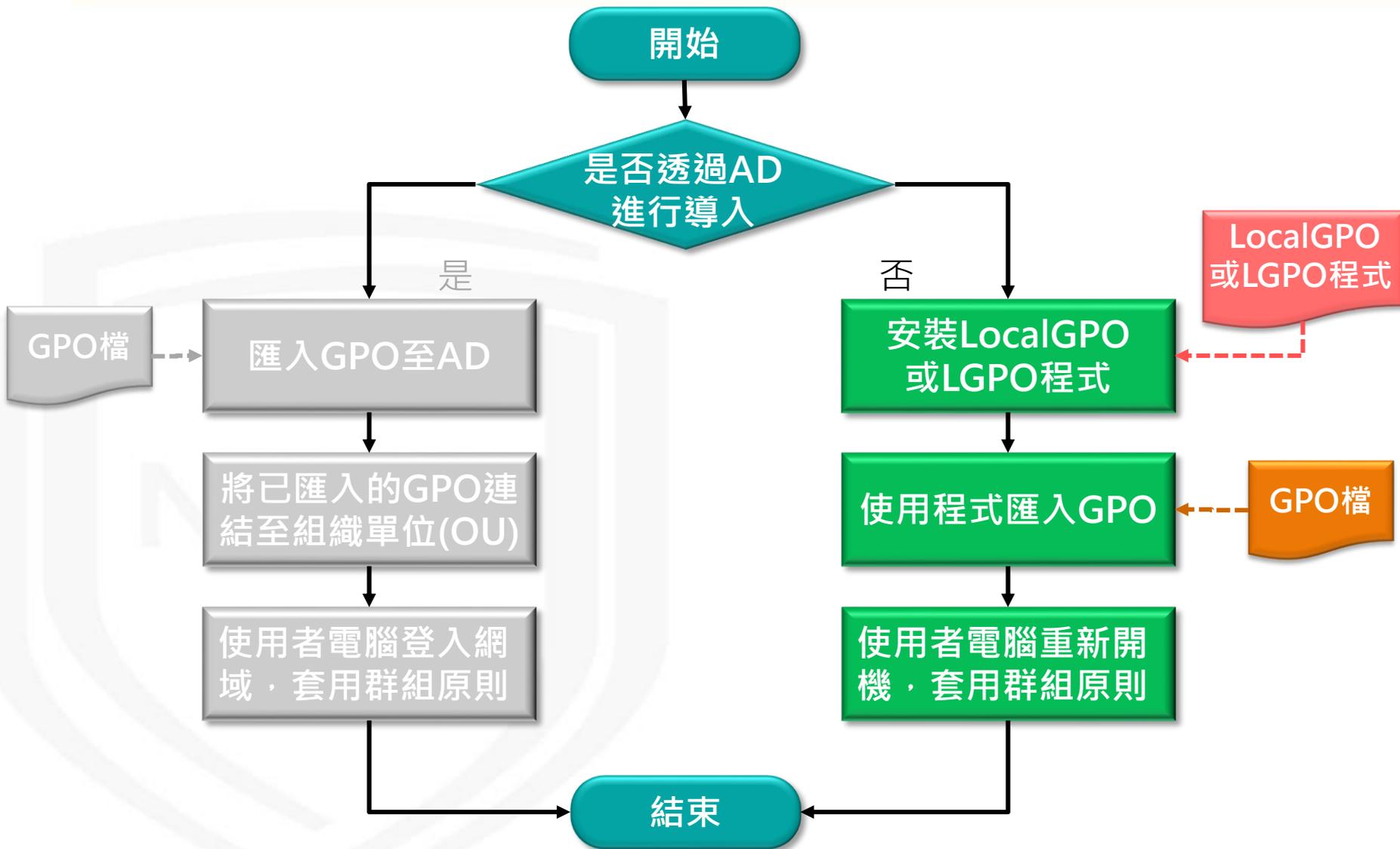
The screenshot shows the Group Policy Management console with the following elements:

- Left Pane:** A tree view showing the hierarchy: 樹系: gcb.gov.tw > 網域 > gcb.gov.tw > 技術服務中心 > 群組原則物件. The GPO 'Windows10AccountSettings' is selected and highlighted with a red box and a red circle labeled '1'.
- Right Pane:** The 'Windows10AccountSettings' properties window. The '連結' (Link) tab is active. The '在這個位置顯示連結(L):' dropdown is set to 'gcb.gov.tw'. Below it, a list of linked sites, domains, and OUs is shown.
- Dialog Box:** A confirmation dialog box is open, asking '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 red circle labeled '3'.
- Annotations:**
 - A red box and circle labeled '2' highlights the '檢測評鑑組' (Detection and Assessment Group) folder in the left pane.
 - A red arrow points from the 'Windows10AccountSettings' GPO to the '檢測評鑑組' folder.
 - A yellow arrow points from the 'Windows10AccountSettings' GPO to the '確定' button in the dialog box.
 - A blue speech bubble with yellow text says '請拖曳 GPO 至 組織單位' (Please drag the GPO to the organizational unit).
 - A blue speech bubble with yellow text says '請點選 GPO 進行 拖曳' (Please click the GPO to drag).

使用單機導入GCB

NCCST

GCB導入流程

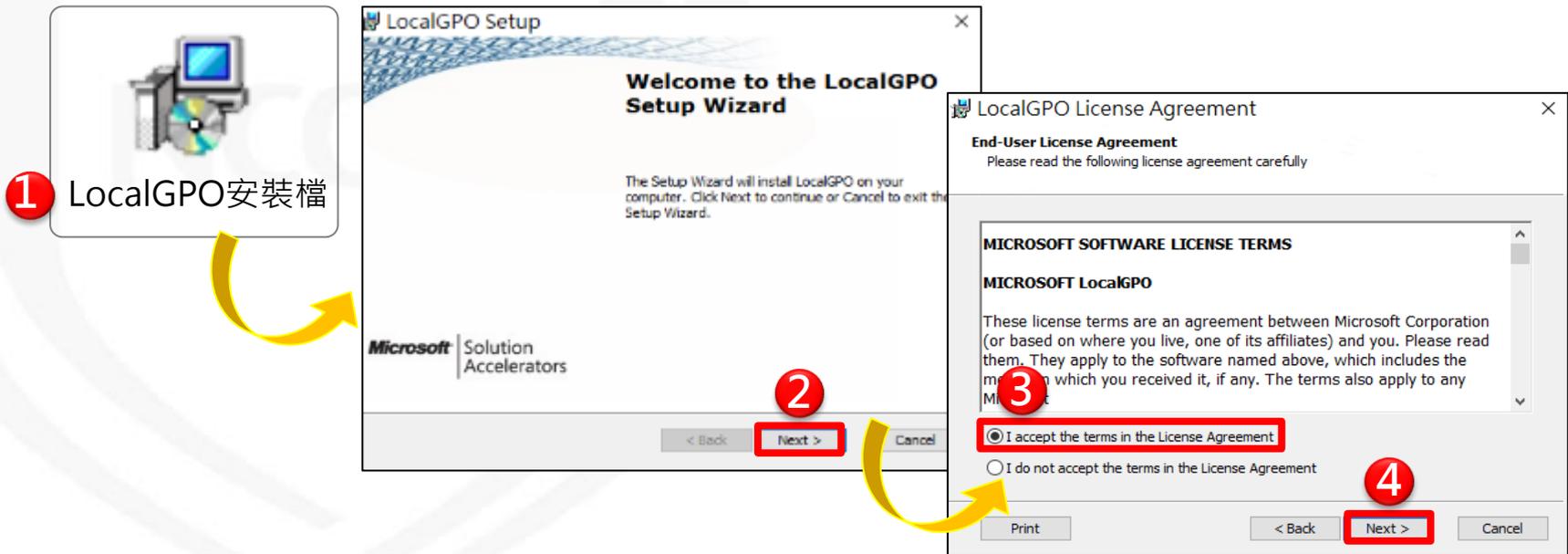


使用LocalGPO程式導入GCB

NCCST

安裝LocalGPO程式(1/2)

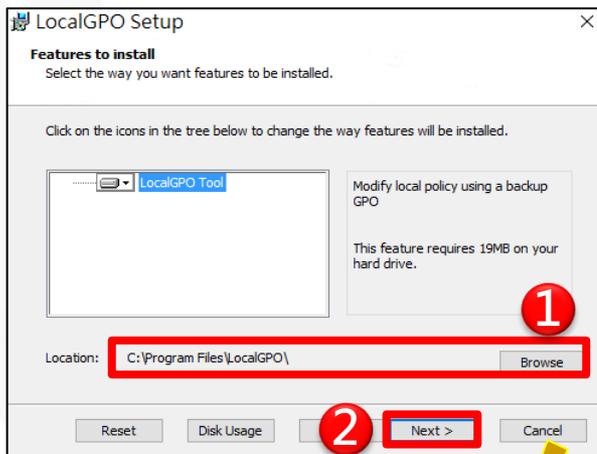
- 執行「LocalGPO」安裝檔
- 在Welcome to the LocalGPO Setup Wizard頁面→點選「Next」
- 在End-User License Agreement頁面→勾選接受授權協議→點選「Next」



The image shows two overlapping windows from the LocalGPO installation process. The background window is the 'LocalGPO Setup' wizard, titled 'Welcome to the LocalGPO Setup Wizard'. It contains instructions to click 'Next' to continue. A red box highlights the 'Next >' button, with a yellow arrow pointing to it from a red circle labeled '2'. The foreground window is the 'LocalGPO License Agreement' dialog, titled 'End-User License Agreement'. It displays the 'MICROSOFT SOFTWARE LICENSE TERMS' for 'MICROSOFT LocalGPO'. A red box highlights the radio button for 'I accept the terms in the License Agreement', with a yellow arrow pointing to it from a red circle labeled '3'. Another red box highlights the 'Next >' button at the bottom of the license agreement window, with a yellow arrow pointing to it from a red circle labeled '4'. A separate box on the left shows a computer icon and a CD-ROM icon, with a red circle labeled '1' and the text 'LocalGPO安裝檔' (LocalGPO installation file). A yellow arrow points from this box to the 'LocalGPO Setup' window.

安裝LocalGPO程式(2/2)

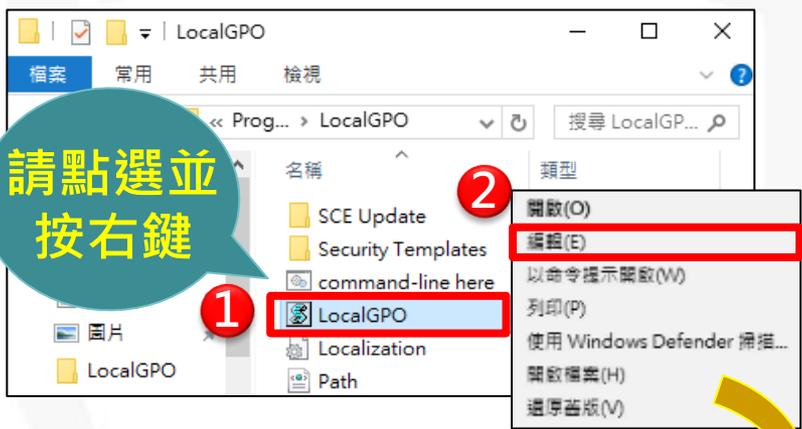
- 在Features to Install頁面→確認安裝路徑→點選「Next」
- 在Ready to Install頁面→點選「Install」進行安裝
- 點選「是」，允許安裝LocalGPO在這部電腦上
- 點選「Finish」完成安裝作業



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 = "1") then
    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(strOpVer,3) = "6.0") and (strProductType <> "1") then
    strOS = "Win8"
Elseif(Left(strOpVer,3) = "6.0") and (strProductType = "1") then
    strOS = "WS08R2"
Elseif(Left(strOpVer,3) = "6.0") 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) = "6.0") and (strProductType = "1") then
    strOS = "WS03"
Elseif(Left(strOpVer,3) = "5.1") 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
    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

1. LocalGPO Command-line (highlighted with a red box and callout: 請點選並按右鍵)

2. 以系統管理員身分執行 (highlighted with a red box and callout: 請點選以管理員身分執行)

Windows 系統

- Windows Defender
- Windows PowerShell

Windows 附屬應用程式

檔案總管

3. FFC0-4763-AD67-F9B2125C54DA (highlighted with a red circle and callout: 複製GPO所在路徑)

DomainSy

Backup

gpreport

```
選取系統管理員: LocalGPO Command-line

cscript LocalGPO.wsf /Path:C:\GPObackups\ /Compare
- Compares Local Policy configuration to the contents of a GPO Backup.

cscript LocalGPO.wsf /Path:C:\GPObackups /Export /GPOPack
- Creates a GPOPack and stores it in the specified path. GPOPacks
can be copied to other computers, and applied by double-clicking
GPOPack.wsf.

cscript LocalGPO.wsf /Path:C:\GPObackups\ /MLGPO:Users
- Applies the contents of the GPO Backup stored in the specified
path to the specified Multiple Local Group Policy Object (MLGPO).

cscript LocalGPO.wsf /Restore
- Restores the entire Local Policy to its default configuration.

C:\Program Files\LocalGPO>
微軟注音 半 :
```

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

```
1 系統管理員: LocalGPO Command-line
C:\Program Files\LocalGPO>cscript LocalGPO.wsf /path:C:\Users\Admin\Desktop\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}
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.

Applied valid INF from C:\Users\Admin\Desktop\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}
No valid Machine POL to apply in C:\Users\Admin\Desktop\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}
No valid User POL to apply in C:\Users\Admin\Desktop\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}
No valid Audit Policy CSV to apply in C:\Users\Admin\Desktop\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}

Local Policy Modified!

Please restart the computer to refresh the Local Policy

微軟注音 半 :
```

輸入語法與路徑

路徑不能有空白

顯示修改成功

```
2 系統管理員: LocalGPO Command-line
Local Policy Modified!

Please restart the computer to refresh the Local Policy

C:\Program Files\LocalGPO>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。

微軟注音 半 :
```

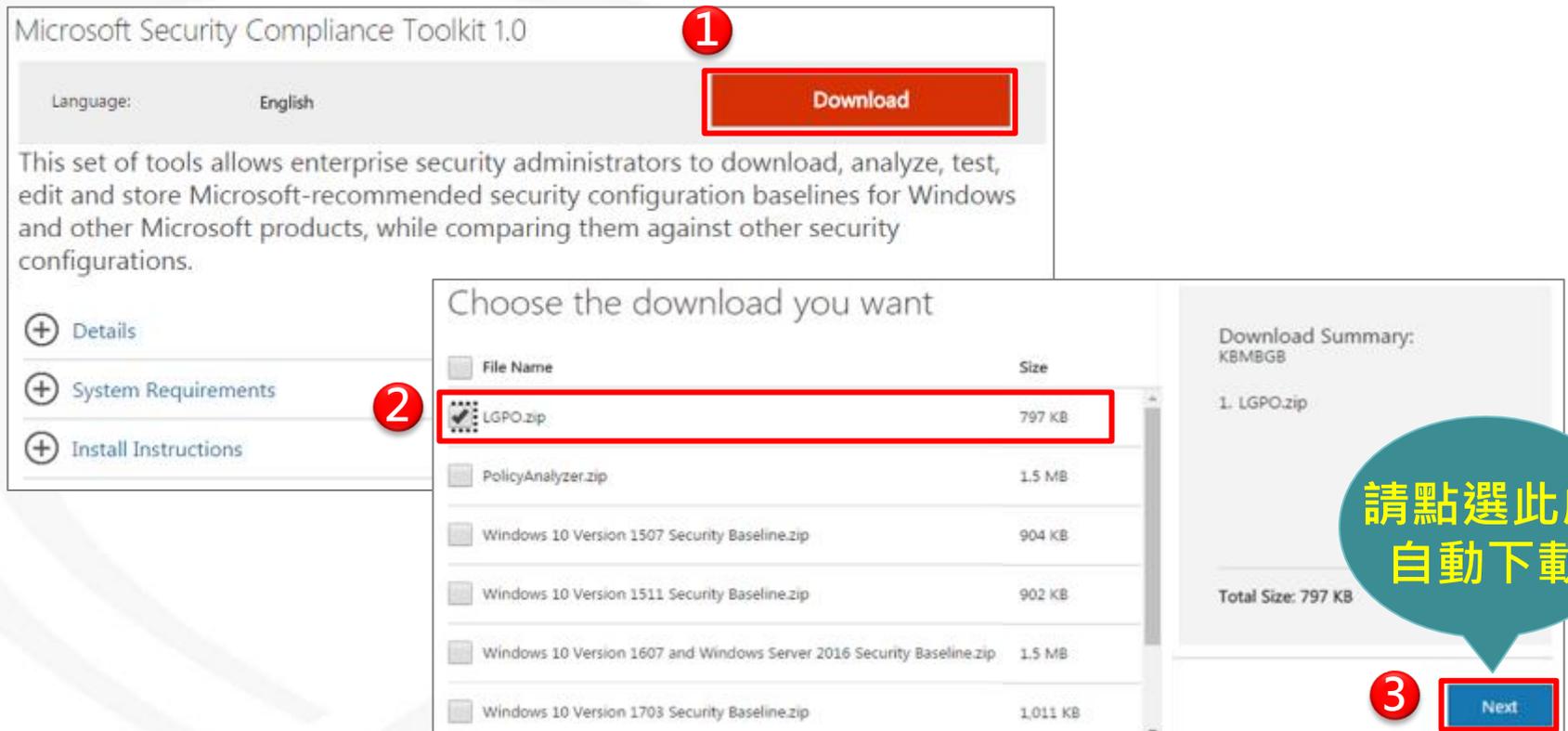
輸入語法更新或重新開機

使用LGPO程式導入GCB

NCCST

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>



Microsoft Security Compliance Toolkit 1.0

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

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

+ Details
+ System Requirements **2**
+ Install Instructions

Choose the download you want

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

Download Summary:
KBMBGB
1. LGPO.zip
Total Size: 797 KB

3 [Next](#)

請點選此處自動下載

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>

1 命令提示字元

請點選並按右鍵

2 以系統管理員身分執行(A)

請點選以管理員身分執行

3 FC0-4763-AD67-F982125C54DA

4 cd C:\Users\Admin\Desktop\LGPO

輸入切換路徑語法

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

```
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation. 著作權所有，並保留部分權利。

C:\Users\Admin\Desktop\LGPO>LGPO.exe /b C:\Users\Admin\Desktop\
LGPO.exe v2.2 - Local Group Policy Object utility

Creating LGPO backup in "C:\Users\Admin\Desktop\{F92B0D00-D642-49F4-A69B-D56CBCFC8560}"

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

輸入備份語法

1

顯示備份結果

```
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation. 著作權所有，並保留部分權利。

C:\Users\Admin\Desktop\LGPO>cd C:\Users\Admin\Desktop\LGPO

C:\Users\Admin\Desktop\LGPO>LGPO.exe /g C:\Users\Admin\Desktop\
Windows10ComputerSettings\Windows10ComputerSettings(Other)\
{7E9C934E-DE0F-4716-BD4A-6AC1C2813AF4}
LGPO.exe v2.2 - Local Group Policy Object utility

Apply security template: C:\Users\Admin\Desktop\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{7E9C934E-DE0F-4716-BD4A-6AC1C2813AF4}\DomainSysvol\GPO\Machine\Windows nt\SecEdit\GptTmpl.inf

Import Machine settings from registry.pol: C:\Users\Admin\Desktop\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{7E9C934E-DE0F-4716-BD4A-6AC1C2813AF4}\DomainSysvol\GPO\Machine\registry.pol

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

輸入匯入語法

2

顯示匯入結果

檢查GPO套用狀況之方式

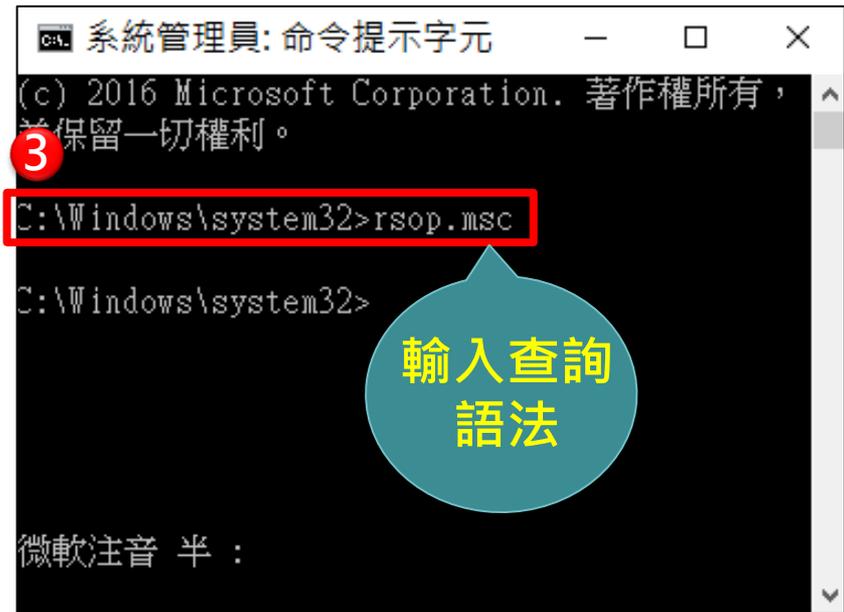
NCCST

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

正在處理原則結果組...

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

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

正在處理，請稍候

選擇項目	設定
模式	記錄
使用者名稱	GCB\test
顯示使用者原則設定值	是
電腦名稱	GCB_3_WIN10
顯示電腦原則設定值	是

進度:

顯示群組
原則套用
結果

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

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



1 請點選並按右鍵

2 請點選以管理員身分執行

3 輸入查詢語法

```
Microsoft Windows [版本 10.0.10586]
(c) 2016 Microsoft Corporation. 著作權所有
並保留一切權利。
C:\Windows\system32>gpresult /h C:\Users\test\Desktop\GPO.html
正在產生報告 ...
```

AD環境下的檢查方式(4/4)

- 使用Gpresult檢查群組原則，顯示如下



1 GPO.html

群組原則結果		
GCB\3_WIN10 的 GCB\test		
資料收集: 2017/12/15 下午 02:50:18		
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
使用可感知的加密來存放密碼	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
密碼嚴格使用期限	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
帳戶鎖定閾值	5 次無效的登入嘗試	Windows10AccountSettings

2

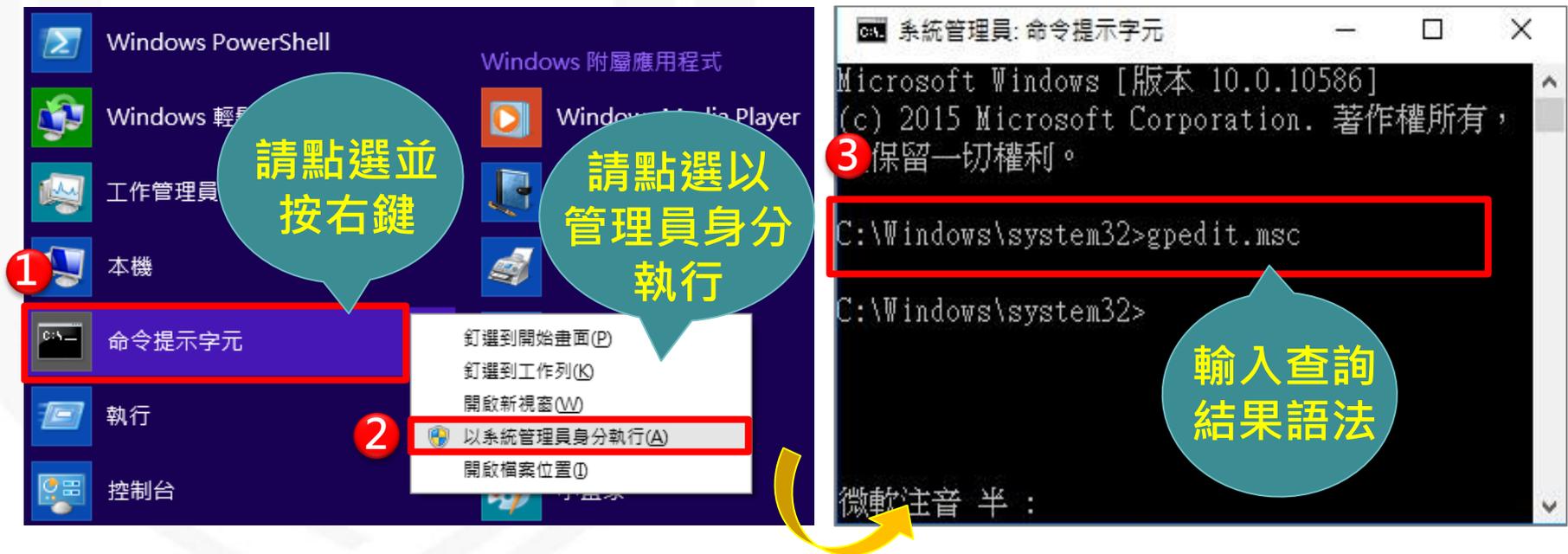
原則	設定	優勢 GPO
使用可感知的加密來存放密碼	已停用	Windows10AccountSettings
密碼必須符合複雜性需求	已啟用	Windows10AccountSettings
密碼長度最小值	8 個字元	Windows10AccountSettings
密碼最長使用期限	90 天	Windows10AccountSettings
密碼嚴格使用期限	1 天	Windows10AccountSettings
強制密碼歷程記錄	已記憶 3 個密碼	Windows10AccountSettings
帳戶原則/帳戶鎖定原則		
隱藏		
原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分鐘	Windows10AccountSettings
帳戶鎖定期間	15 分鐘	Windows10AccountSettings
帳戶鎖定閾值	5 次無效的登入嘗試	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

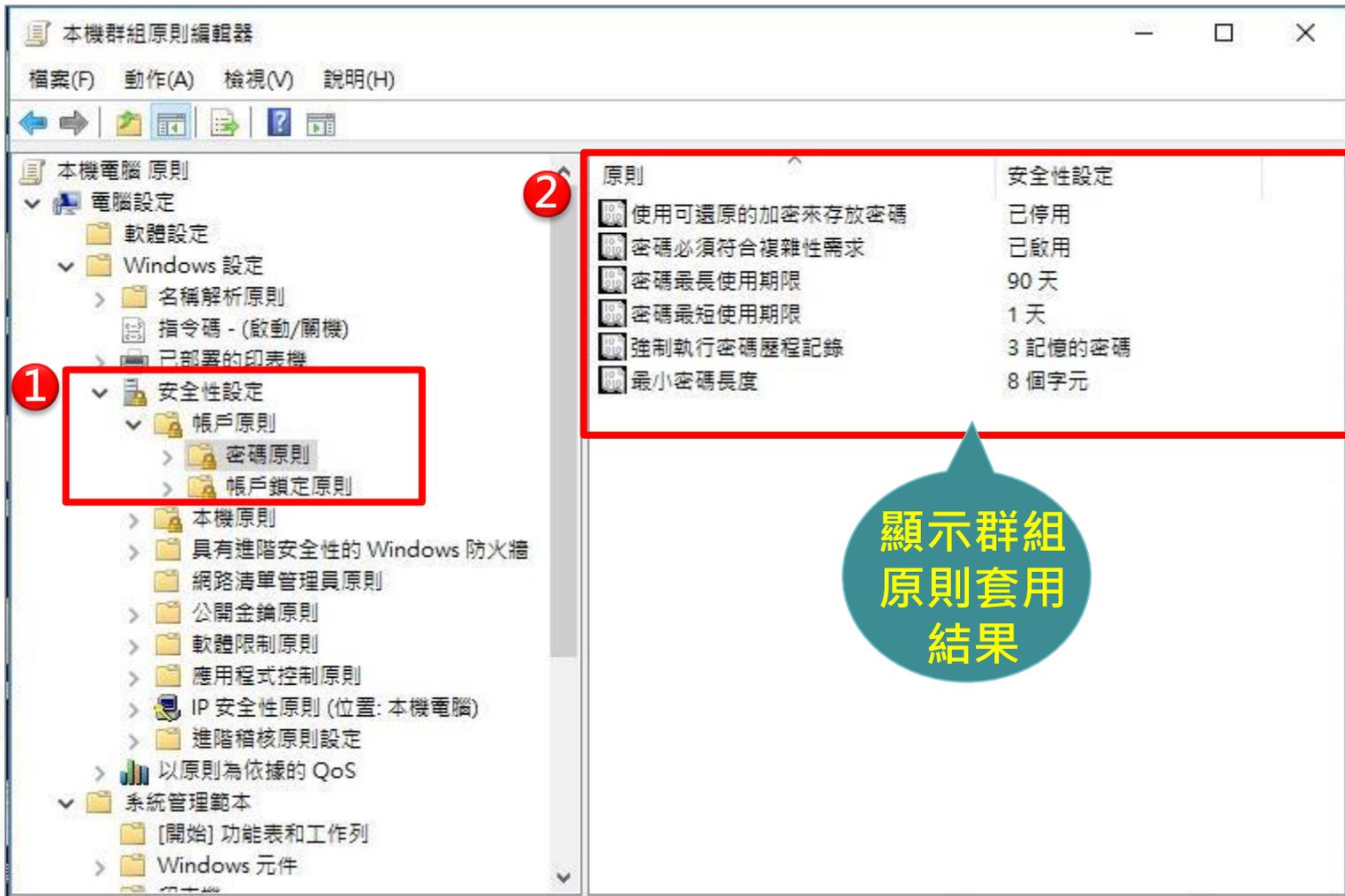
- 點選「Command-line」按滑鼠**右鍵**→選擇「以系統管理員身分執行」
- 於「Command-line」輸入Gpedit.msc



The image shows a Windows Start menu search for '命令提示字元' (Command Prompt). A red box highlights the search result, with a callout bubble saying '請點選並按右鍵' (Please click and right-click). A second red box highlights the context menu option '以系統管理員身分執行(A)' (Run as administrator), with a callout bubble saying '請點選以管理員身分執行' (Please click to run as administrator). A yellow arrow points from this menu to a screenshot of the Command Prompt window. In the Command Prompt, the command 'C:\Windows\system32>gpedit.msc' is entered and highlighted with a red box, with a callout bubble saying '輸入查詢結果語法' (Enter query result syntax). The Command Prompt window title is '系統管理員: 命令提示字元' (System Administrator: Command Prompt).

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

1 安全性設定

帳戶原則

密碼原則

帳戶鎖定原則

本機原則

具有進階安全性的 Windows 防火牆

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)

進階稽核原則設定

以原則為依據的 QoS

系統管理範本

[開始] 功能表和工作列

Windows 元件

2 原則

原則	安全性設定
<input type="checkbox"/> 使用可還原的加密來存放密碼	已停用
<input type="checkbox"/> 密碼必須符合複雜性需求	已啟用
<input type="checkbox"/> 密碼最長使用期限	90 天
<input type="checkbox"/> 密碼最短使用期限	1 天
<input type="checkbox"/> 強制執行密碼歷程記錄	3 記憶的密碼
<input type="checkbox"/> 最小密碼長度	8 個字元

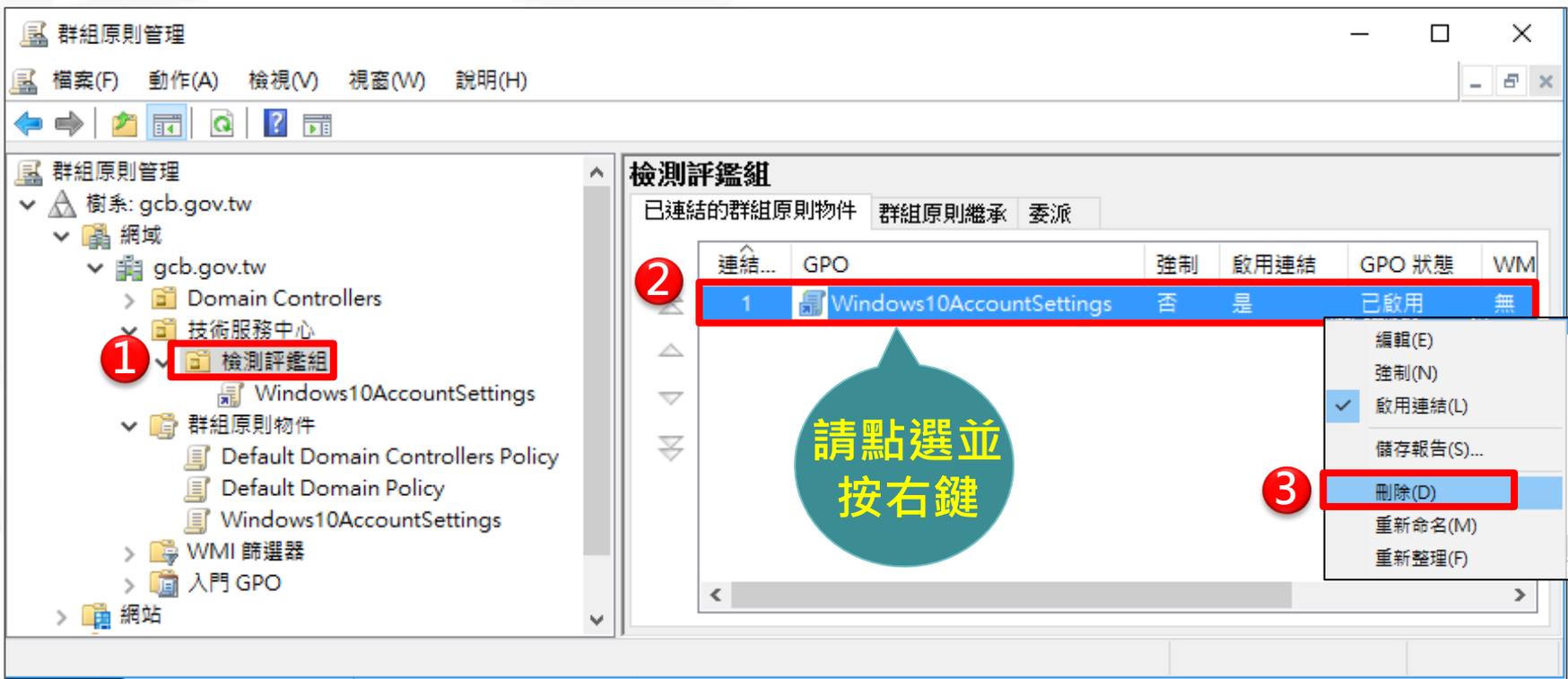
顯示群組原則套用結果

恢復原始設定之方式

NCCST

AD環境下恢復原始設定方式

- 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

The image shows a Windows context menu for 'LocalGPO Command-line' and a screenshot of the command prompt. The context menu has three callouts: 1. '請點選並按右鍵' (Please click and right-click) pointing to the 'LocalGPO Command-line' item. 2. '請點選以管理員身分執行' (Please click to run as administrator) pointing to the '以系統管理員身分執行(A)' option. 3. '輸入恢復原始設定語法' (Enter the syntax for restoring original settings) pointing to the command prompt. The command prompt shows the command `cscript LocalGPO.wsf /Restore` and the output: 'Local Policy default values restored!' and 'Please restart the computer to refresh the Local Policy'. A fourth callout '顯示結果' (Show results) points to the output text.

1 請點選並按右鍵

2 請點選以管理員身分執行

3 輸入恢復原始設定語法

顯示結果

```
C:\Program Files\LocalGPO>cscript LocalGPO.wsf /Restore
Microsoft (R) Windows Script Host Version 5.012
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

微軟注音 半 :les\LocalGPO>
```

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設定値

NCCST

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

NCCST

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)

The screenshot illustrates the process of creating a test Organizational Unit (OU) in Active Directory. It is divided into six numbered steps:

- 1**: In the Windows System Management Tools window, the "Active Directory Users and Computers" icon is highlighted with a red box.
- 2**: A callout bubble with the text "請點選並按右鍵" (Click and right-click) points to the "技術服務中心" (Technical Service Center) folder in the left-hand tree view.
- 3**: A context menu is opened over the "技術服務中心" folder, and the "新增(N)" (New) option is highlighted with a red box.
- 4**: A sub-menu is displayed, and the "組織單位" (Organizational Unit) option is highlighted with a red box.
- 5**: The "新增物件 - 組織單位" (New Object - Organizational Unit) dialog box is shown. The "名稱(A):" (Name) field contains "測試組織" (Test Organization) and is highlighted with a red box.
- 6**: The "確定" (OK) button at the bottom of the dialog box is highlighted with a red box.

Additional callouts include "建立測試用之組織單位" (Create test organizational unit) pointing to the name field in step 5.

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)

The screenshot shows the Active Directory console window titled "Active Directory 使用者和電腦". The left pane shows the tree structure with "gcb.gov.tw" expanded, and "測試組織" (Test Organization) selected. The right pane shows a table of objects:

名稱	類型	描述
3_WIN10	電腦	
userA	使用者	

Annotations and steps:

- 1: "技術服務中心" (Technical Service Center) is selected in the left pane.
- 2: "3_WIN10" and "userA" are selected in the right pane.
- 3: "測試組織" (Test Organization) is selected in the left pane.
- 4: The "是(Y)" (Yes) button is clicked in the warning dialog box.

Warning dialog box text:

Active Directory 網域服務

移動 Active Directory 網域服務中的物件，會使您現有的系統無法按照設計好的方式運作。例如，移動組織單位 (OU) 會影響對 OU 內的帳戶套用群組原則的方式。

您確定要移動這些物件嗎？

在這個嵌入的單元開啟時不要顯示這個警告(D)

是(Y) 否(N)

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

請點選並按右鍵

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

- 網域
 - gcb.gov.tw
 - Domain Controller
 - 技術服務中心
 - 群組原則物件**
 - Default Domain Controllers Policy
 - Default Domain Policy
 - WMI 篩選器
 - 入門 GPO
 - 網站
 - 群組原則模型
 - 群組原則結果

gcb.gov.tw 中的 群組原則物件

名稱	GPO 狀態	WMI 篩選器
Default Domain Control...	已啟用	無
Default Domain Policy	已啟用	無

新增 GPO

名稱(N): TestWindows10AccountSettings

來源入門 GPO(S): (無)

確定 取消

1 2 3 4

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

歡迎使用【匯入設定精靈】

您可以從任何 GPO 備份將設定匯入。匯入設定不會修改其他 GPO 屬性、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，或是，從您繼承做為群組原則管理操作，執行本機群組原則管理。

請按 [下一步 (N) >]

匯入設定精靈

備份 GPO

備份這個 GPO 目前的設定。

匯入設定將永久刪除這個 GPO 的目前設定，建議您先備份這個 GPO。

備份 (A)...

< 上一步 (B) > [下一步 (N) >]

匯入設定精靈

備份位置

選取匯入設定的來源備份資料夾。

備份資料夾 (A):

ator\Desktop\GCB-Windows10-gpos\Windows10AccountSettings

[瀏覽 (R)...]

請點選 GPO 檔案位置

匯入設定精靈

來源 GPO

選取匯入設定的來源 GPO。

已備份的 GPO (A):

名稱	時間戳記	描述	領域
Windows10AccountSet...	2017/12/15 下午 0...		GCB.G

只顯示每個 GPO 最新的版本 (S)

[檢視設定 (V)...]

< 上一步 (B) > [下一步 (N) >] [取消] [說明]

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

匯入設定精靈

掃描備份
精靈正在掃描在備份中的設定，決定是否有任何安全性主體或 UNC 路徑需要轉移。

掃描結果:
備份不包含任何安全性主體或 UNC 路徑的參照，請按 [下一步]

1

< 上一步(B) 下一步(N) >

匯入設定精靈

正在完成 匯入設定精靈

您已成功地完成 [匯入設定精靈]，精靈將繼續。

摘要:
備份位置: C:\Users\Administrator\Desktop\
備份 GPO: Windows10AccountSettings...
名稱: Windows10AccountSettings...
時間戳記: 2017/12/15 下午 02:55:00
描述:

請按一下 [完成] 來關閉這個精靈並匯入。

2

< 上一步(B) 完成

匯入

匯入進度:

狀態(S):
GPO: Windows10AccountSettings... 已成功

顯示匯入成功

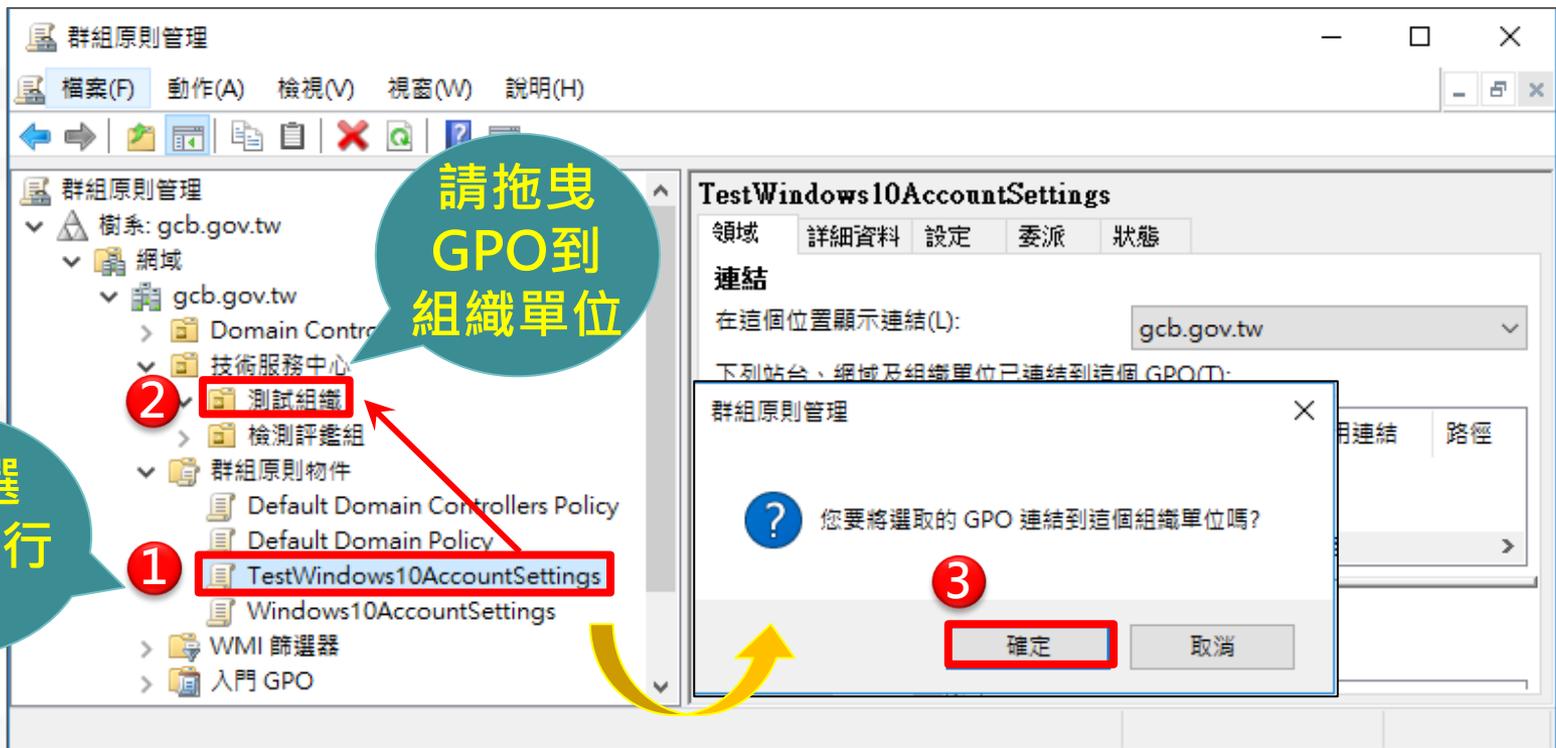
3

確定 取消

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)



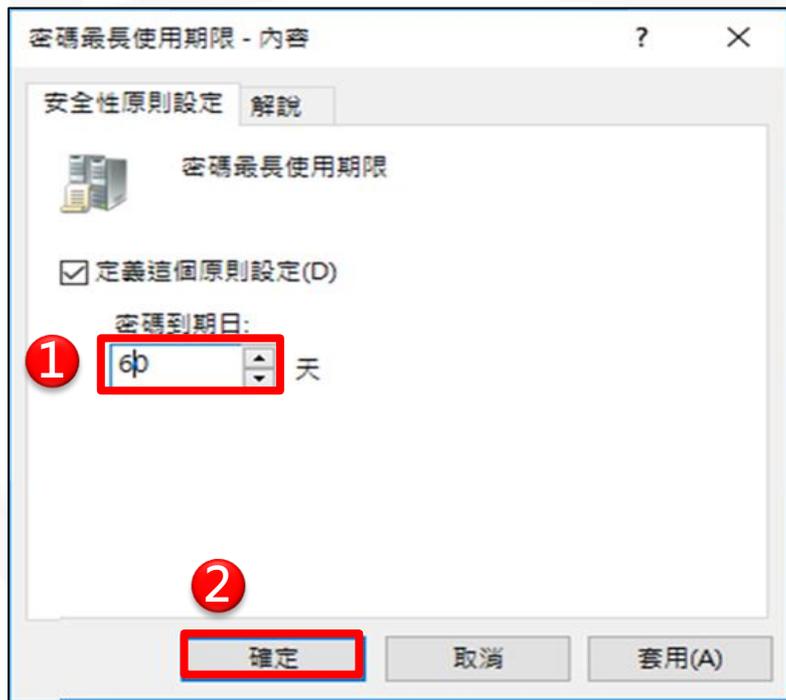
- 在測試群組原則物件節點按滑鼠**右鍵**→選擇「編輯」
- 調整組態之設定值
 - 開啟「群組原則管理編輯器」→點選「電腦設定」→點選「原則」→點選「系統管理範本」→點選「TestWin10AccountSettings」，選擇組態進行調整

The screenshot shows two windows from the Group Policy Management console:

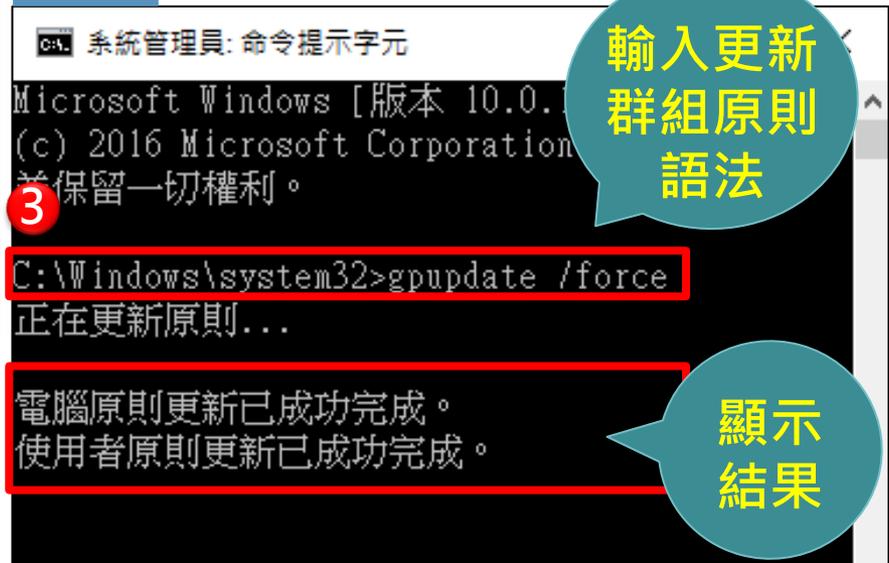
- Left Window (Group Policy Management):** Shows the hierarchy: Group Policy Objects (GPOs) for the domain gcb.gov.tw. The 'TestWindows10AccountSettings' GPO is selected, and the context menu is open. A red box highlights the 'Edit(E)...' option, with a callout bubble saying '點選按右鍵' (Click right button) and a red circle with the number '1'.
- Right Window (Group Policy Management Editor):** Shows the configuration for the 'TestWindows10AccountSettings' GPO. The 'Computer Configuration' > 'Policies' > 'System Management Templates' path is followed. The 'TestWin10AccountSettings' template is selected, and the 'Security Settings' > 'Account Policies' > 'Password Policy' path is followed. A red box highlights the 'Password Policy' folder, with a callout bubble saying '點選進行修改' (Click to modify) and a red circle with the number '3'. The 'Password Maximum Age' policy is selected, and its value is set to '90 天'. A red box highlights this value, with a callout bubble saying '點選進行修改' (Click to modify) and a red circle with the number '4'.

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



使用者電腦CMD畫面



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

Active Directory 使用者和電腦

群組原則管理

gcb.gov.tw 中的 群組原則物件

名稱	GPO 狀態	WMI 篩選器
Default Domain Control...	已啟用	無
Default Domain Policy	已啟用	無

請點選並按右鍵

測試對象拖曳回該組織單位

1 2 3 4 5 6

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

The image shows two screenshots of Windows Group Policy Management tools. The left screenshot is the Group Policy Management console, and the right is the Group Policy Editor.

Left Screenshot (Group Policy Management):

- Tree view: 樹系: gcb.gov.tw > 網域 > gcb.gov.tw > 群組原則物件 > 例外管理
- Right pane: 編輯(E)... (highlighted with a red box and circled with a '2')
- Callout: 點選按右鍵 (1) (highlighted with a red box and circled with a '1')

Right Screenshot (Group Policy Editor):

- Tree view: 電腦設定 > Windows 設定 > 安全性設定 > 密碼原則 (highlighted with a red box and circled with a '3')
- Right pane: 密碼最長使用期限 (highlighted with a red box and circled with a '4'), set to 90 天
- Callout: 點選進行修改 (highlighted in a blue speech bubble)

A yellow arrow points from the '例外管理' node in the left screenshot to the '密碼原則' node in the right screenshot.

單機環境下調整與測試GCB

NCCST

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



1 .NET Framework 安裝檔



2



3

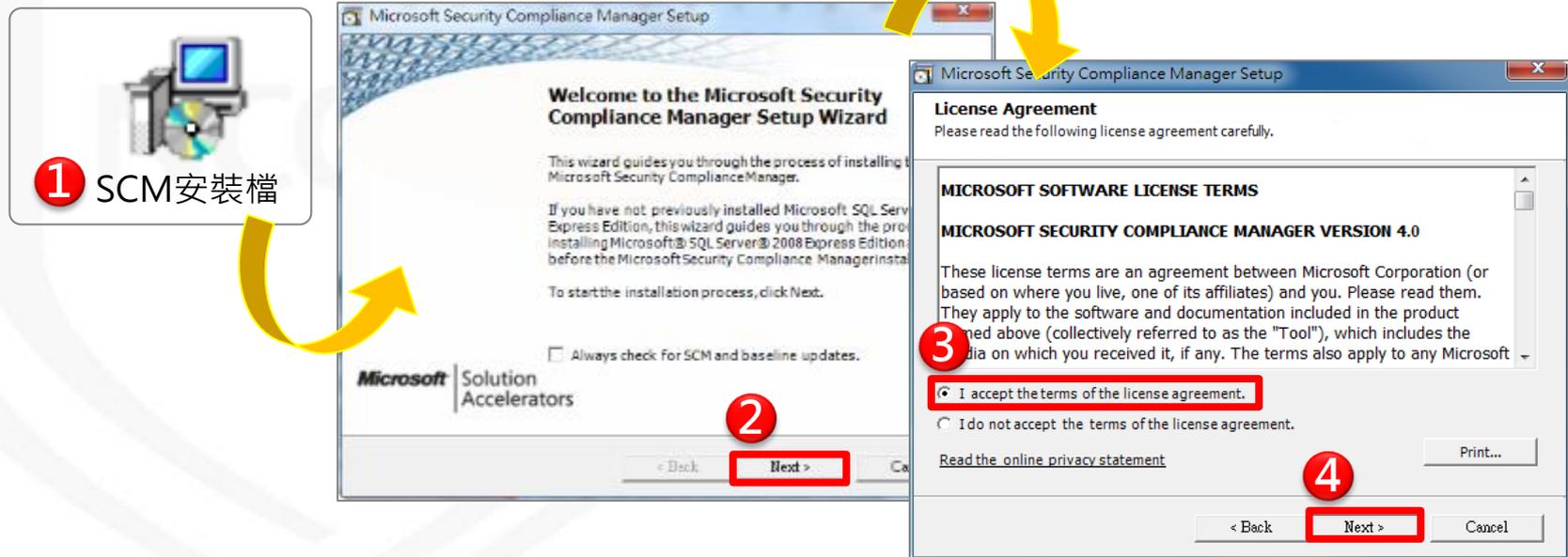
4



5

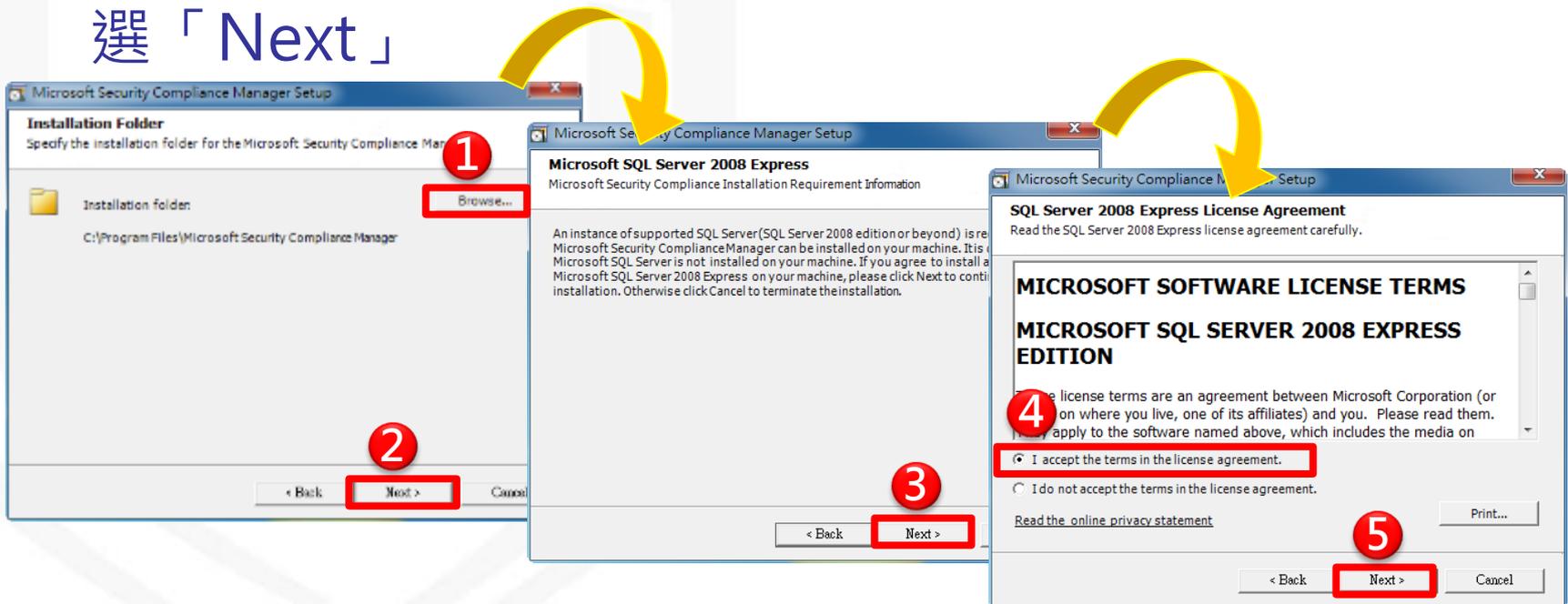
安裝SCM(1/3)

- 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)

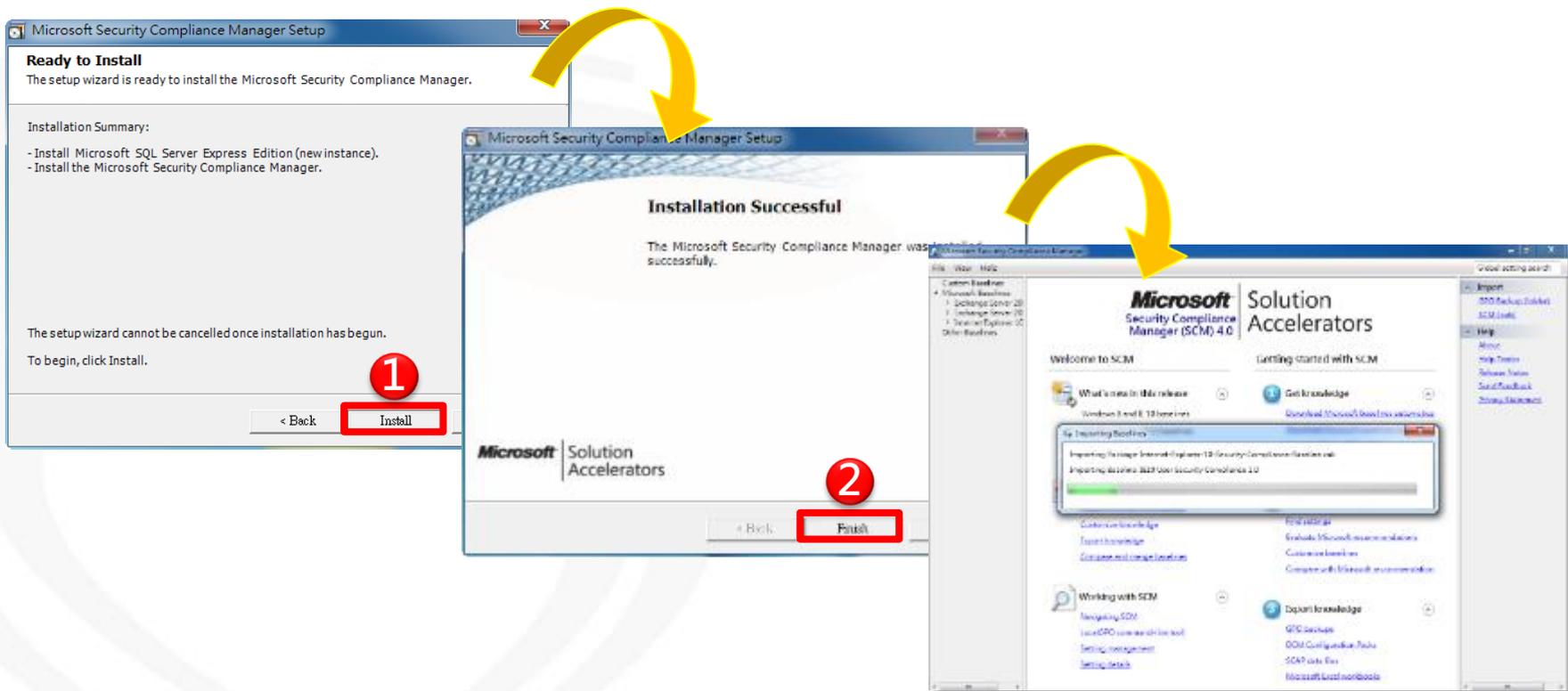
- 在Installation Folder頁面→確認安裝路徑→點選「Next」
- 開始安裝SQL Server 2008 Express→點選「Next」
- 在License Agreement頁面→勾選接受授權協議→點選「Next」



安裝SCM(3/3)



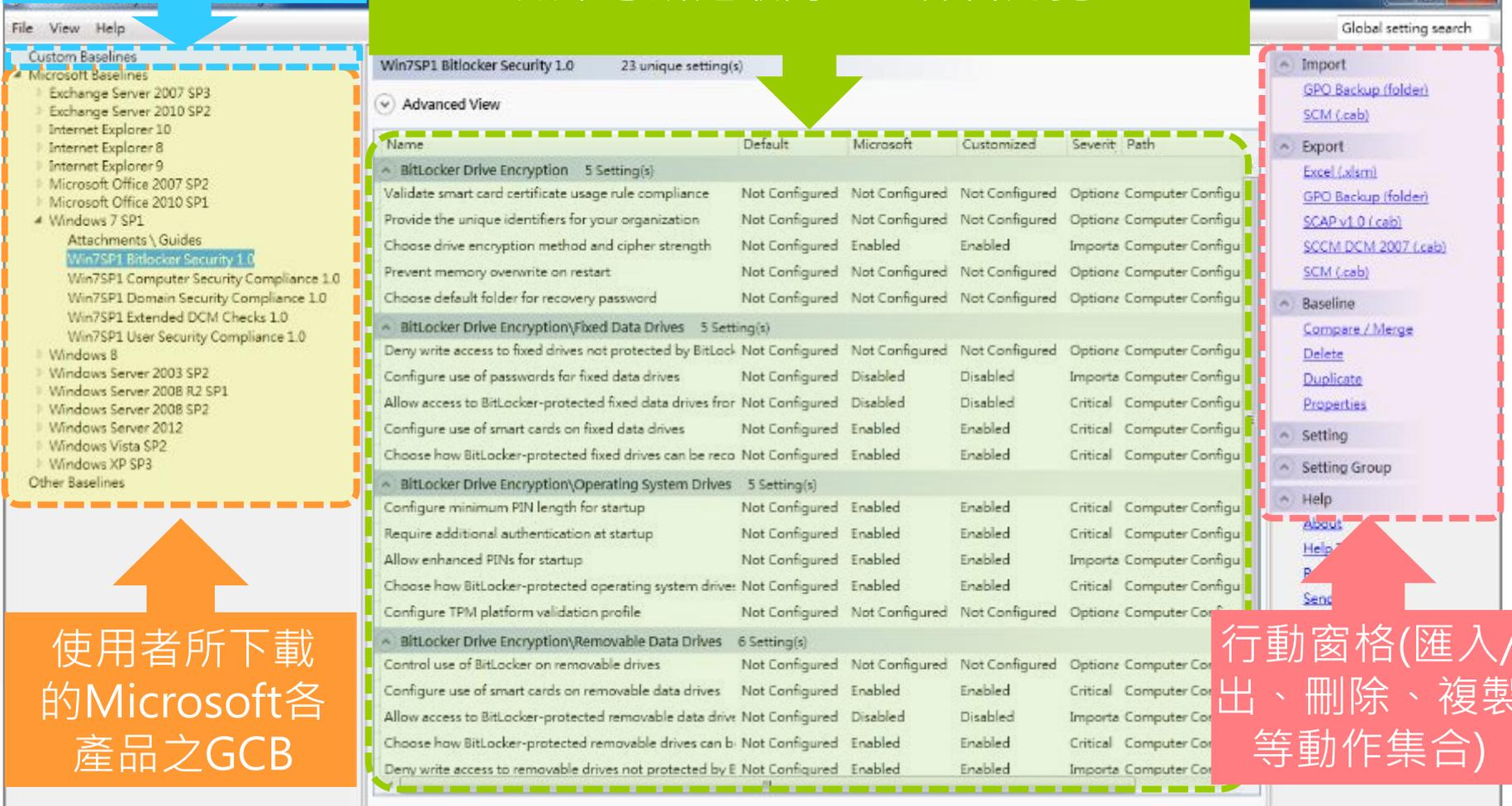
- 在Read to Install頁面→點選「Install」安裝SCM
- 在Installation Successful頁面→點選「Finish」



SCM畫面說明

客製化GCB

顯示您所選取的GCB條目總覽



The screenshot displays the SCM interface with three main components:

- Left Panel (Custom Baselines):** A tree view showing various Microsoft Baselines. The selected baseline is "Win7SP1 BitLocker Security 1.0".
- Center Panel (Advanced View):** A table showing 23 unique settings for the selected baseline. The table has columns for Name, Default, Microsoft, Customized, Severity, and Path.
- Right Panel (Global setting search):** A context menu with options like Import, Export, Baseline, Setting, and Help.

Name	Default	Microsoft	Customized	Severity	Path
BitLocker Drive Encryption 5 Setting(s)					
Validate smart card certificate usage rule compliance	Not Configured	Not Configured	Not Configured	Options	Computer Configu
Provide the unique identifiers for your organization	Not Configured	Not Configured	Not Configured	Options	Computer Configu
Choose drive encryption method and cipher strength	Not Configured	Enabled	Enabled	Imports	Computer Configu
Prevent memory overwrite on restart	Not Configured	Not Configured	Not Configured	Options	Computer Configu
Choose default folder for recovery password	Not Configured	Not Configured	Not Configured	Options	Computer Configu
BitLocker Drive Encryption\Fixed Data Drives 5 Setting(s)					
Deny write access to fixed drives not protected by BitLock	Not Configured	Not Configured	Not Configured	Options	Computer Configu
Configure use of passwords for fixed data drives	Not Configured	Disabled	Disabled	Imports	Computer Configu
Allow access to BitLocker-protected fixed data drives fro	Not Configured	Disabled	Disabled	Critical	Computer Configu
Configure use of smart cards on fixed data drives	Not Configured	Enabled	Enabled	Critical	Computer Configu
Choose how BitLocker-protected fixed drives can be reco	Not Configured	Enabled	Enabled	Critical	Computer Configu
BitLocker Drive Encryption\Operating System Drives 5 Setting(s)					
Configure minimum PIN length for startup	Not Configured	Enabled	Enabled	Critical	Computer Configu
Require additional authentication at startup	Not Configured	Enabled	Enabled	Critical	Computer Configu
Allow enhanced PINs for startup	Not Configured	Enabled	Enabled	Imports	Computer Configu
Choose how BitLocker-protected operating system drive:	Not Configured	Enabled	Enabled	Critical	Computer Configu
Configure TPM platform validation profile	Not Configured	Not Configured	Not Configured	Options	Computer Configu
BitLocker Drive Encryption\Removable Data Drives 6 Setting(s)					
Control use of BitLocker on removable drives	Not Configured	Not Configured	Not Configured	Options	Computer Co
Configure use of smart cards on removable data drives	Not Configured	Enabled	Enabled	Critical	Computer Co
Allow access to BitLocker-protected removable data driv	Not Configured	Disabled	Disabled	Imports	Computer Co
Choose how BitLocker-protected removable drives can b	Not Configured	Enabled	Enabled	Critical	Computer Co
Deny write access to removable drives not protected by E	Not Configured	Enabled	Enabled	Imports	Computer Co

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」

Microsoft Security Compliance Manager

File View Help

Custom Baselines

- Microsoft Baselines
 - Exchange Server 2007 SP3
 - Exchange Server 2010 SP2
 - Internet Explorer 10
 - Internet Explorer 8
 - Internet Explorer 9
 - Microsoft Office 2007 SP2
 - Microsoft Office 2010 SP1
 - Windows 7 SP1
 - Windows 8
 - Windows Server 2003 SP2
 - Windows Server 2008 R2 SP2
 - Windows Server 2008 SP2
 - Windows Server 2012
 - Windows Vista SP2
 - Windows XP SP3
 - Windows 10 version 1607
 - Windows Server 2016
 - Windows 10 version 1511
 - Windows Server 2012 R2
 - Windows 8.1
 - Internet Explorer 11
 - Microsoft Office 2013
 - SQL Server 2012
- Other Baselines

Microsoft Security Compliance Manager (SCM) 4.0

Solution Accelerators

Welcome to SCM

Getting started with

1 Get knowledge

- Download Microsoft Security Baselines
- Download Microsoft Security Baselines
- Import a Microsoft Security Baseline
- Import a Group Policy

2 Customize knowledge

- Find settings
- Evaluate Microsoft Security Baselines
- Customize baseline
- Compare with Microsoft Security Baselines

Import

- GPO Backup (folder)
- SCM (.cab)

瀏覽資料夾

Import GPO Backup (folder)

網路

控制台

資源回收筒

Windows10AccountSettings

{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}

DomainSysvol

GPO

Machine

User

Windows10ComputerSettings

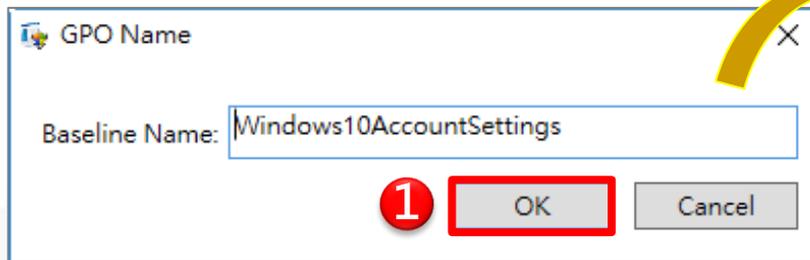
3 確定 取消

須選擇至機碼資料夾

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



Microsoft Security Compliance Manager

File View Help

Custom Baselines

 GPO Import

 Attachments \ Guides

 Windows10AccountSettings 0.0

Microsoft Baselines

 Exchange Server 2007 SP3

 Exchange Server 2010 SP2

 Internet Explorer 10

 Windows 7

 Windows 8

 Windows 8.1

 Windows 10 version 1607

 Windows 10 version 1511

 Windows Server 2008 R2 SP1

 Windows Server 2008 SP2

 Windows Server 2012

 Windows Vista SP2

 Windows XP SP3

 Windows 10 version 1607

 Windows Server 2016

 Windows 10 version 1511

 Windows Server 2012 R2

 Windows 8.1

 Internet Explorer 11

 Microsoft Office 2013

 SQL Server 2012

Other Baselines

Windows10AccountSettings 0.0 9 unique setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severity	Path
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy 3 Setting(s)					
Account lockout threshold			5	Critical	Computer Configuration\Windows
Reset account lockout counter after			15	Critical	Computer Configuration\Windows
Account lockout duration			15	Critical	Computer Configuration\Windows
Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy 6 Setting(s)					
Minimum password age			1	Critical	Computer Configuration\Windows
Maximum password age			90	Critical	Computer Configuration\Windows
Minimum password length			8	Critical	Computer Configuration\Windows
Password must meet complexity requirements			Enabled	Critical	Computer Configuration\Windows
Enforce password history			3	Critical	Computer Configuration\Windows
Store passwords using reversible encryption			Disabled	Critical	Computer Configuration\Windows

Import

 GPO Backup (folder)

 SCM (.cab)

Export

 Excel (.xlsm)

 GPO Backup (folder)

 SCAP v1.0 (.cab)

 SCCM DCM 2007 (.cab)

 SCM (.cab)

Baseline

 Associate

 Compare / Merge

 Delete

 Duplicate

 Lock

 Properties

Setting

 Add

 Move

Setting Group

匯入的 GPO 清單

顯示匯入的 GPO 項目

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

The screenshot shows the Microsoft Security Compliance Manager interface. On the left, a tree view shows 'Win10-1511 Computer Security Compliance 1.0' selected, with a red box and the number '1' next to it. A callout bubble says '選擇欲匯出的GPO'. In the center, the 'Advanced View' table shows settings for 'Authentication Types'. On the right, the 'Export' menu is open, with 'GPO Backup (folder)' selected, highlighted with a red box and the number '2'. A yellow arrow points from this menu to a 'Export GPO Backup (folder)' dialog box. In this dialog, 'Windows10ComputerSettings' is entered in the name field, highlighted with a red box and the number '4'. A callout bubble says '命名存放GPO的資料夾'. At the bottom of the dialog, '建立新資料夾(M)' is highlighted with a red box and the number '3', and '確定' is highlighted with a red box and the number '5'. The '取消' button is also visible.

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」

Microsoft Security Compliance Manager

Global setting search

Custom Baselines

- Microsoft Baselines
 - Exchange Server 2007 SP3
 - Exchange Server 2010 SP2
 - Internet Explorer 10
 - Internet Explorer 8
 - Internet Explorer 9
 - Microsoft Office 2007 SP2
 - Microsoft Office 2010 SP1
 - Windows 7 SP1
 - Windows 8
 - Windows Server 2003 SP2
 - Windows Server 2008 R2 SP1
 - Windows Server 2008 SP2
 - Windows Server 2012
 - Windows Vista SP2
 - Windows XP SP3
 - Windows 10 version 1607
 - Windows Server 2016
 - Windows 10 version 1511
 - Attachments \ Guides
 - Win10-1511 BitLocker Security 1.0
 - Win10-1511 Credential Guard Security 1.0
 - Win10-1511 Domain Security Compliance 1.0
 - Win10-1511 User Security Compliance 1.0
 - Windows Server 2012 R2
 - Windows 8.1
 - Internet Explorer 11

Win10-1511 Computer Security Compliance 1.0 560 unique setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severit	Path
Authentication Types 40 Setting(s)					
Interactive logon: Require smart ca					
Require digits					
Use Microsoft Passport for Work					
Network access: Let Everyone perm	Disabl				
Maximum PIN length					
Minimum PIN length					
Allow Basic authentication	Disabl				
Interactive logon: Number of previ	10 logor				
Microsoft network client	Disabl				
Network Security					
Allow Basic aut					
Require lower					
Disallow Dige					
Network Secur					

Compare Baselines

Select a baseline from the following list to compare it with 'Win7SP1 User Security Compliance' baseline.

- Custom Baselines
- Microsoft Baselines
 - Exchange Server 2007 SP3
 - Exchange Server 2010 SP2
 - Internet Explorer 10
 - Internet Explorer 8
 - Internet Explorer 9
 - Microsoft Office 2007 SP2
 - Microsoft Office 2010 SP1
 - Windows 7 SP1
- Win7SP1 Computer Security Compliance 1.0
- Win7SP1 Extended DCM Checks 1.0
- Win7SP1 User Security Compliance 1.0
- Windows 8
- Windows Server 2003 SP2
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows Server 2012
- Windows Vista SP2
- Windows XP SP3
- Other Baselines

1 Win10-1511 Computer Security Compliance 1.0

2 Compare / Merge

3 Win7SP1 Computer Security Compliance 1.0

4 OK

同產品 GPO才可合併

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

Compare Baselines

Summary
Baseline A: Win10-1511 Computer Security Compliance 1.0
Baseline B: Win10-1511 User Security Compliance 1.0
Total unique settings compared: 609
Total settings in common: 0
Total settings not in common: 609

Settings that differ (0)

Name	Baseline A	Baseline B	UI Path
------	------------	------------	---------

Settings that match (0)

Name	Baseline A	Baseline B	UI Path
------	------------	------------	---------

Settings only in Baseline A (560)

Settings only in Baseline B (49)

1 Merge Baselines Export to Excel Close

Specify a name for the merged baseline

2 Baseline Name: Merged Baseline

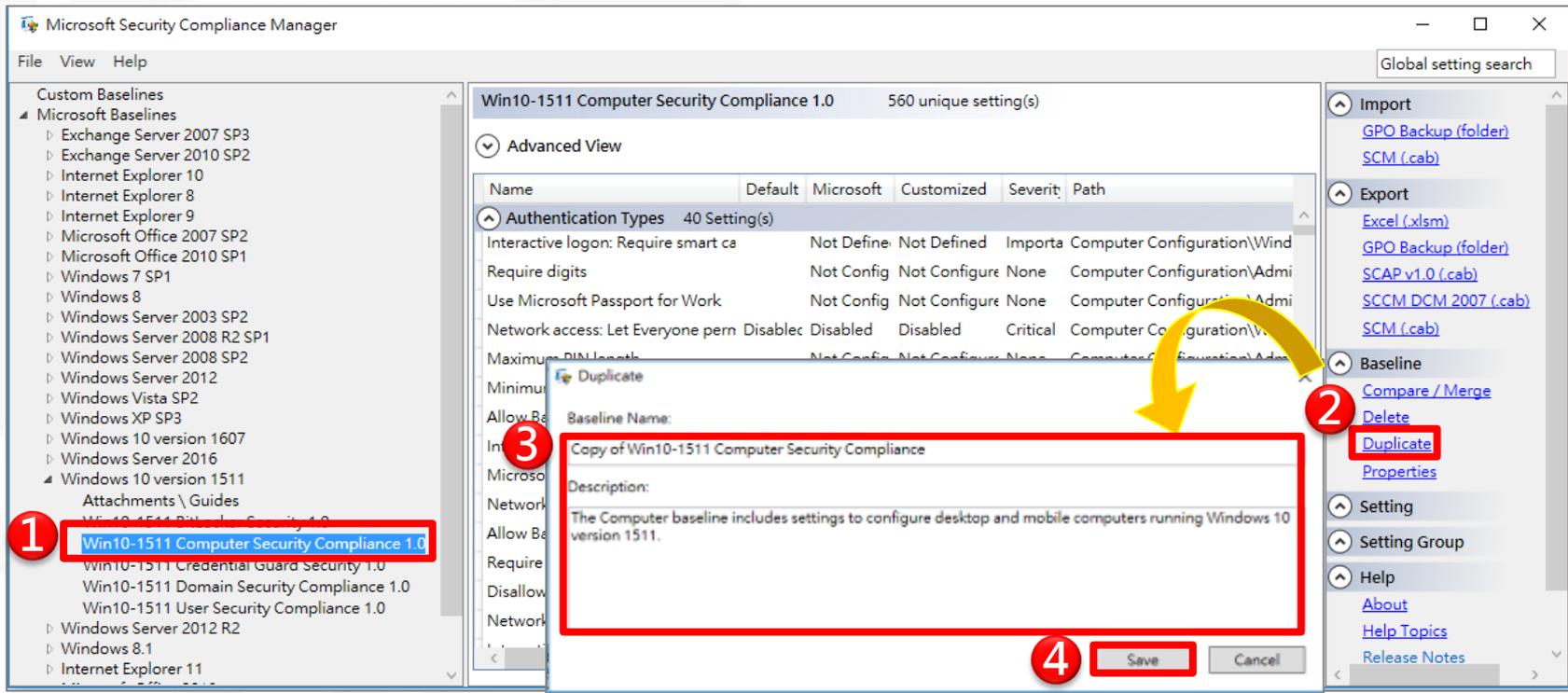
3 OK Cancel

GPO異同處確認

可檢視2個GPO內容

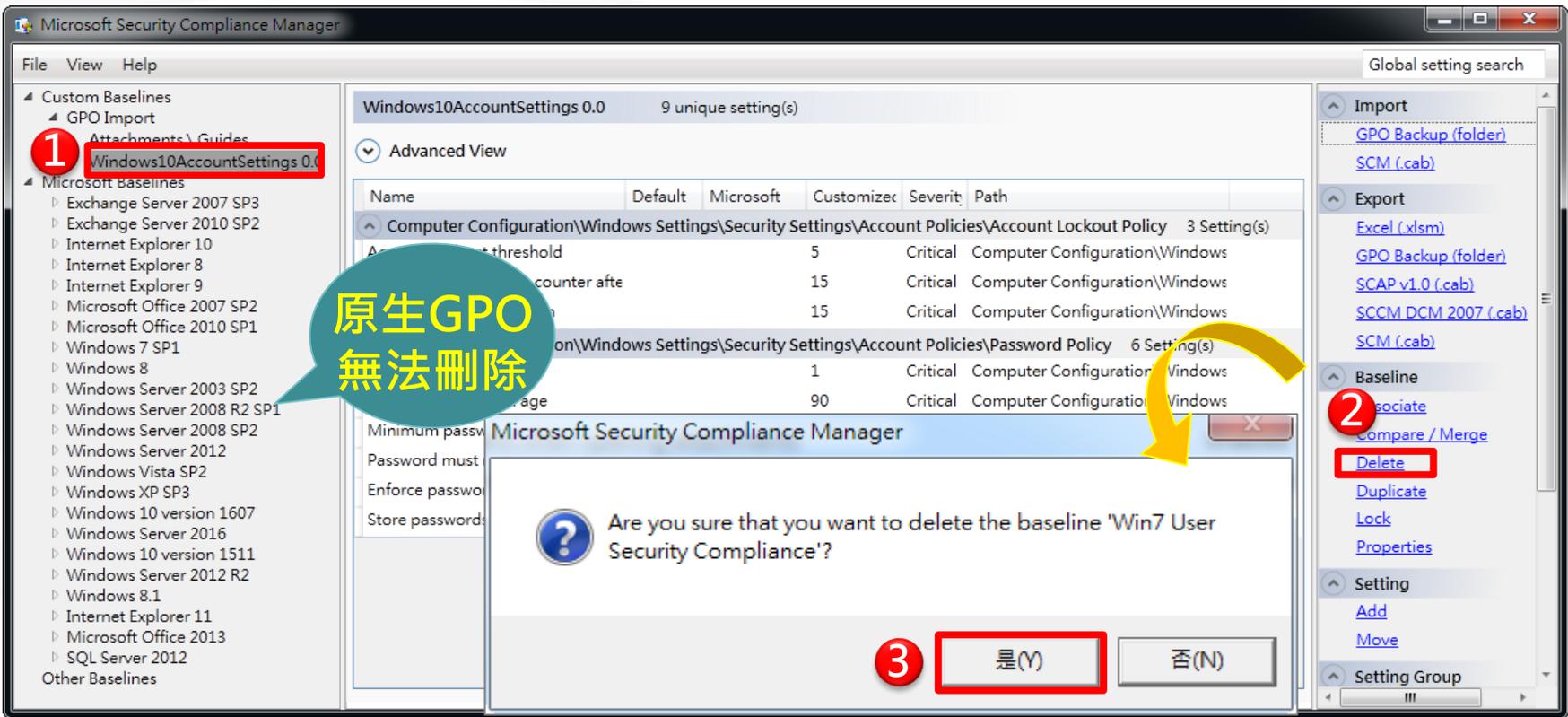
SCM功能介紹-複製GPO檔

- 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



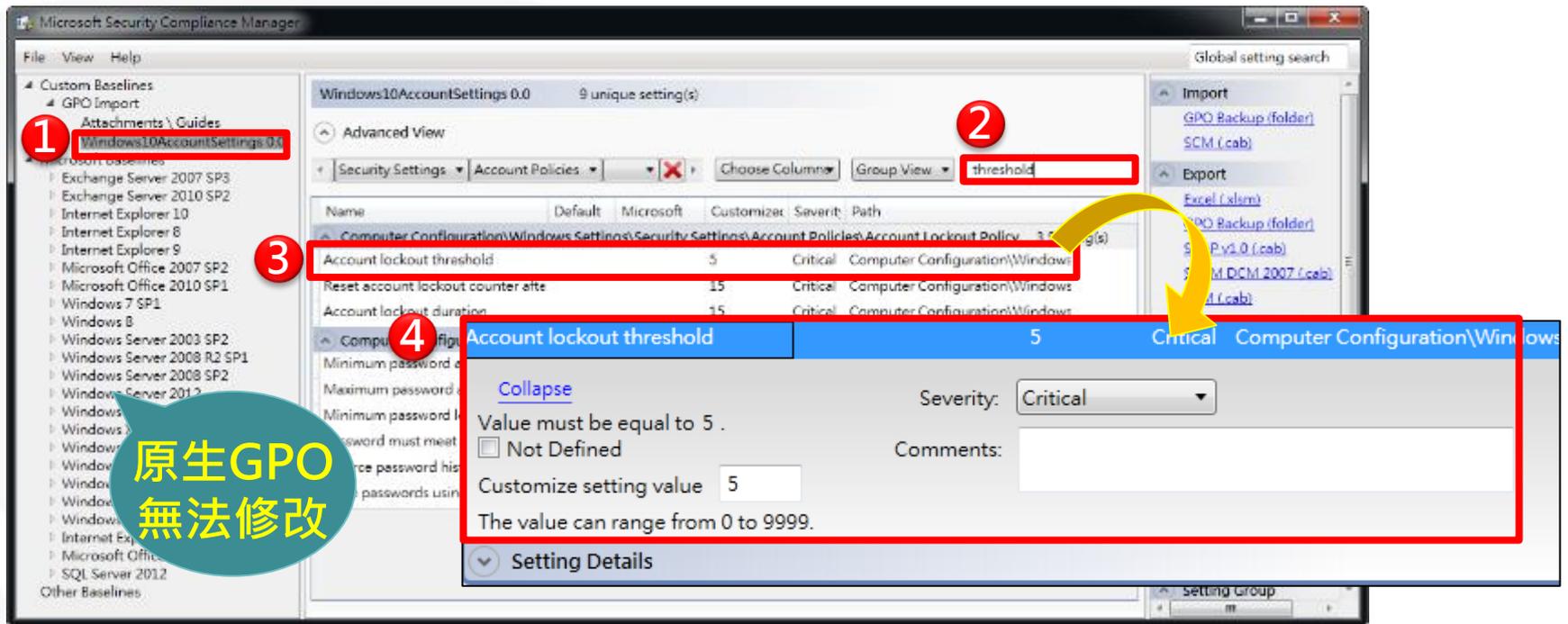
SCM功能介紹-刪除GPO檔

- 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



1. Select the GPO 'Windows10AccountSettings 0.0' in the left pane.

2. Search for 'threshold' in the Advanced View.

3. Select the 'Account lockout threshold' setting.

4. Click on the setting to open the modification dialog.

原生GPO 無法修改

Name	Default	Microsoft	Customize	Severity	Path
Account lockout threshold	5	Critical	Computer Configuration\Windows	Critical	Computer Configuration\Windows

Setting Details: Value must be equal to 5. Customize setting value: 5. Severity: Critical.

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

NCCST