政府組態基準

帳戶原則與精細密碼原則設定說明

(V1.0)

行政院國家資通安全會報技術服務中心

中華民國106年1月

修訂歷史紀錄表

項次	計畫資訊			發行紀錄		說明
	年度	版次	修訂日期	版次	日期	
1	106	V1.0	106/1/5			新編
2						
3						

資料來源：本計畫整理

目次

圖目次

表目次

壹、 前言

一、目的

Windows Server 2003 以前的版本，Active Directory(以下簡稱 AD)伺服器僅能針對網域(Domain)設定單一帳戶原則(包含密碼原則與帳戶鎖定原則)，而自 Windows Server 2008 之後版本為解決此問題，便提供「精細密碼原則」(Fine-Granted Password Policy)之設定方式。

其概念和群組原則物件(GPO)類似，透過容器與物件來設定，惟在精細密碼原則中是以「密碼設定容器(Password Settings Container，以下簡稱 PSC)」及「密碼設定物件(Password Settings Objects，以下簡稱 PSO)」來進行密碼原則設定與套用。

二、適用環境

本文件適用在網域(Domain)環境中，使用網域控制站(Domain Controller)之 AD 伺服器進行控管之微軟公司所發行之作業系統。

三、帳戶原則說明

帳戶原則分為密碼原則與帳戶鎖定原則 2 個類別，共 9 項設定項目，詳見表 1。可透過群組原則物件(Group Policy Object，以下簡稱 GPO)派送與精細密碼原則套用進行原則之設定。

表1　帳戶原則之設定項目列表

項次	類別	原則設定名稱
1	密碼原則	密碼最短使用期限
2		密碼最長使用期限
3		最小密碼長度

4		密碼必須符合複雜性需求
5		強制執行密碼歷程記錄
6		使用可還原的加密來存放密碼
7	帳戶鎖定原則	帳戶鎖定閾值
8		重設帳戶鎖定計數器的時間
9		帳戶鎖定期間

資料來源：本計畫整理

四、文件發行

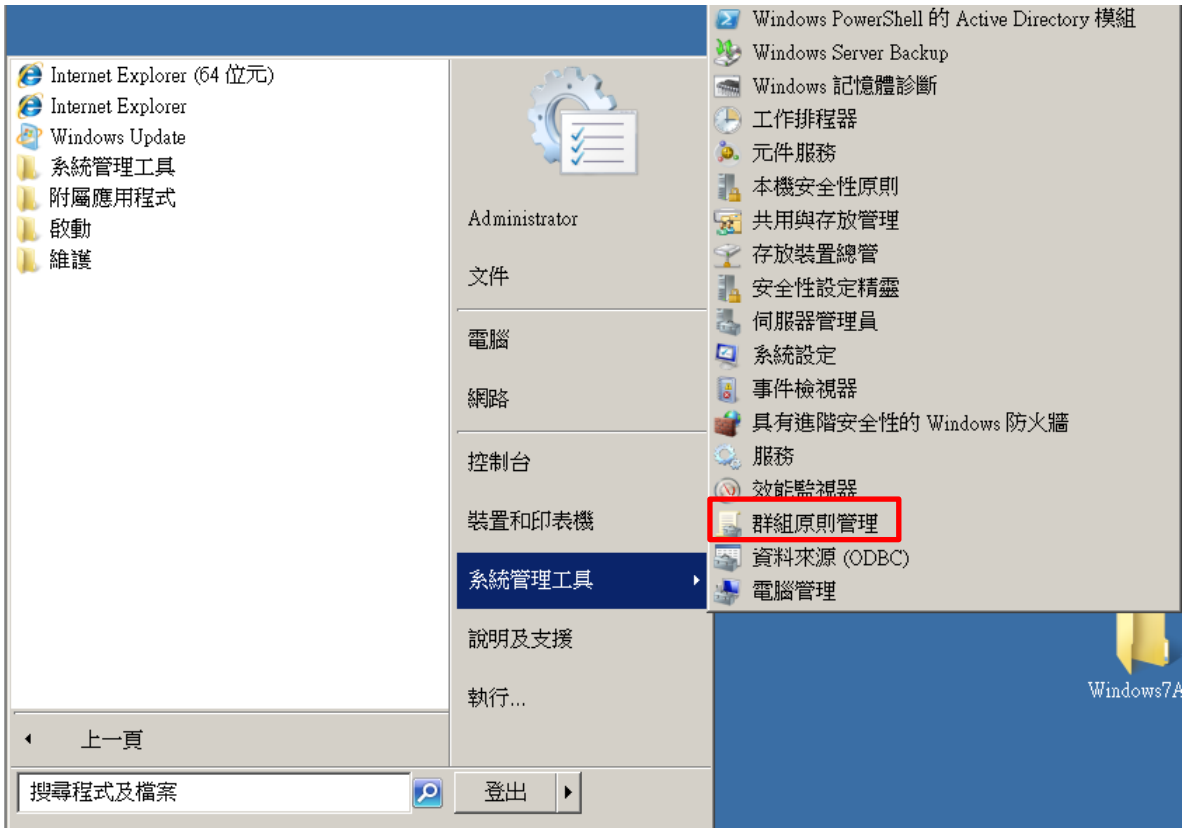
本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為 http://www.nccst.nat.gov.tw/GCB。

貳、 群組原則物件派送部署

在網域環境中，透過 AD 伺服器之群組原則管理功能進行 GPO 派送部署作業，讓控管之使用者電腦與伺服器主機套用群組原則設定。

一、原則設定

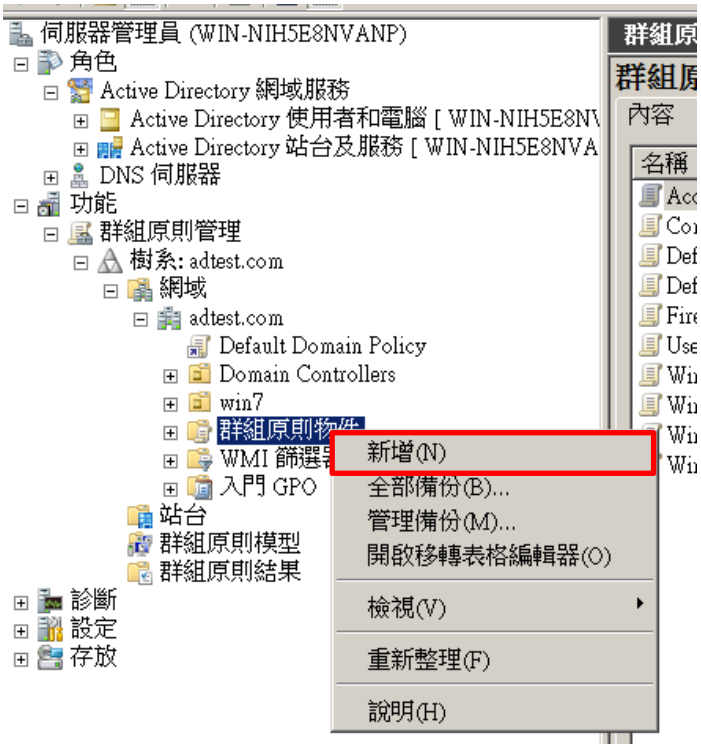
●匯入群組原則物件，點擊「開始」→「所有程式」→「系統管理工具」→「群組原則管理」，詳見圖 1。



資料來源：本計畫整理

圖1　開啟群組原則管理

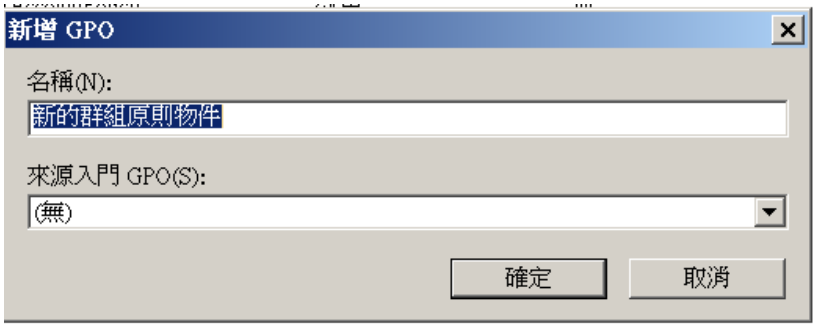
●在「群組原則物件」節點上點選右鍵→選擇「新增」，詳見圖 2。



資料來源：本計畫整理

圖2　新增 GPO

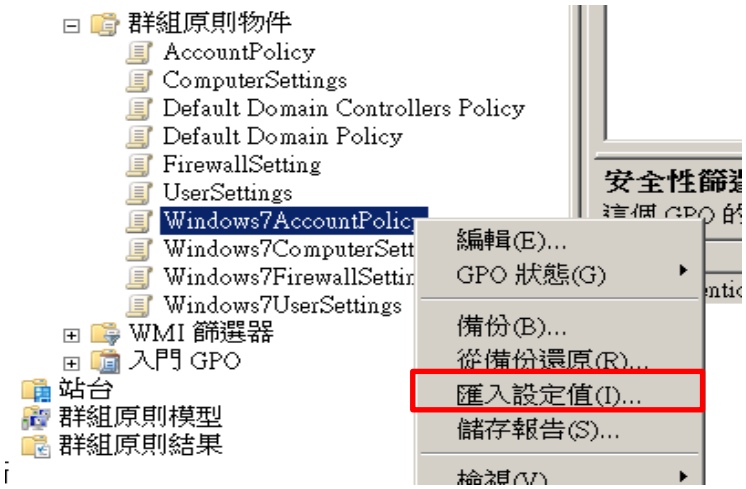
●在「名稱」欄位中輸入 GPO 之名稱，詳見圖 3。



資料來源：本計畫整理

圖3　輸入 GPO 名稱

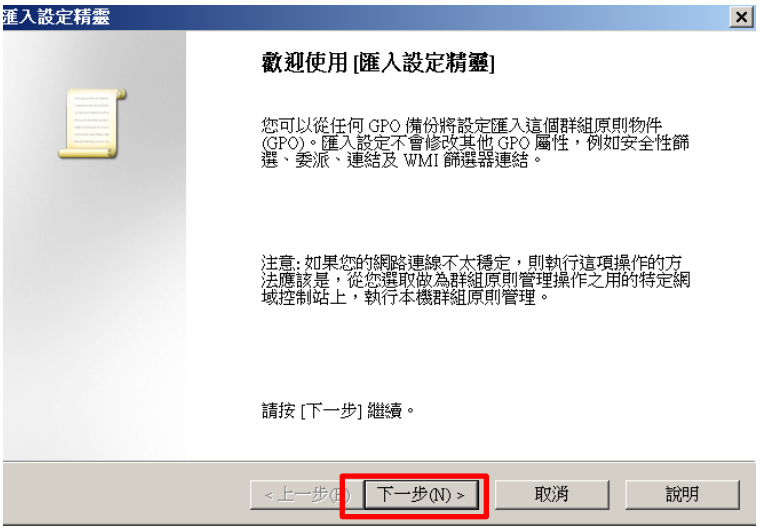
●點選新建的 GPO→選擇「匯入設定值」，詳見圖 4。



資料來源：本計畫整理

圖4　匯入設定值

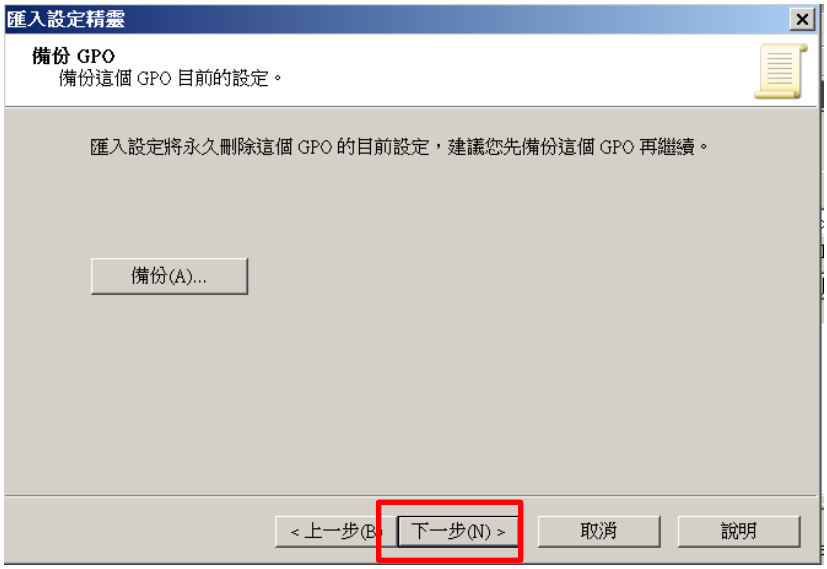
●使用「匯入設定精靈」進行 GPO 之匯入，點選「下一步」，詳見圖 5。



資料來源：本計畫整理

圖5　匯入設定精靈頁面

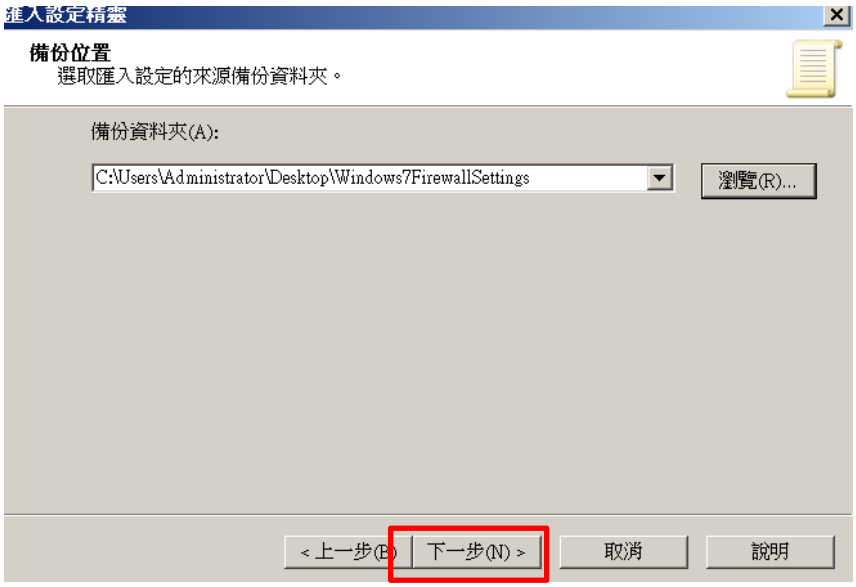
●在備份位置頁面，選取放置 GPO 之資料夾，然後點選「下一步」，詳見圖 6。



資料來源：本計畫整理

圖6　備份位置頁面

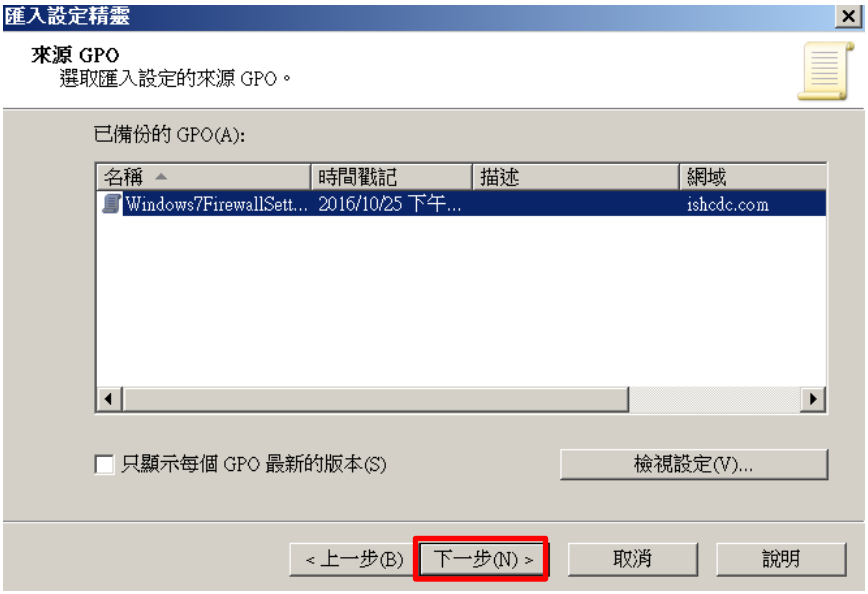
●在來源 GPO 頁面中，選取欲匯入的 GPO 點選「下一步」，詳見圖 7。



資料來源：本計畫整理

圖7　選取 GPO 來源頁面

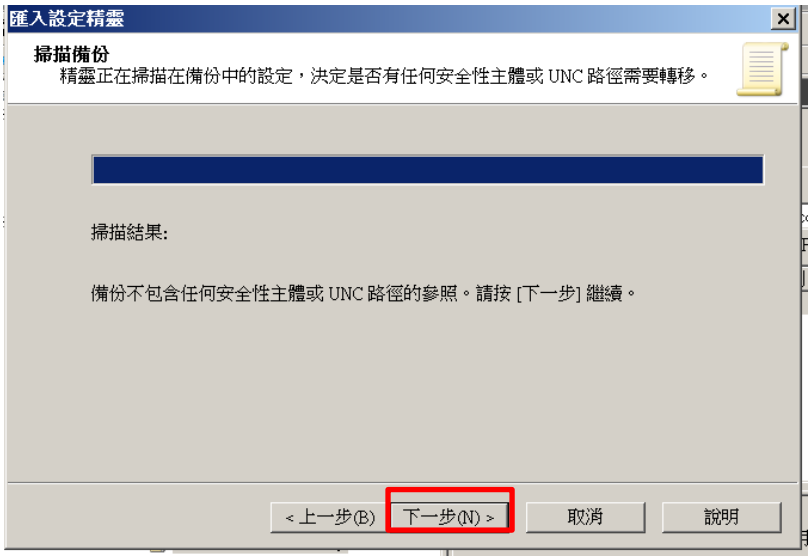
●掃描備份頁面，點選「下一步」，詳見圖 8。



資料來源：本計畫整理

圖8　掃描備份頁面

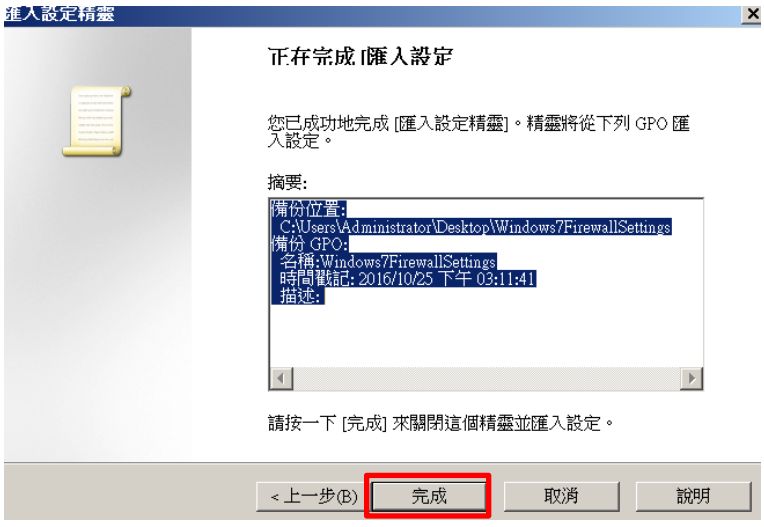
●掃描備份完成後，點選「下一步」，詳見圖 9。



資料來源：本計畫整理

圖9　掃描備份完成頁面

●在匯入進度的頁面，點選「完成」即完成匯入 GPO 之作業，詳見圖 10。

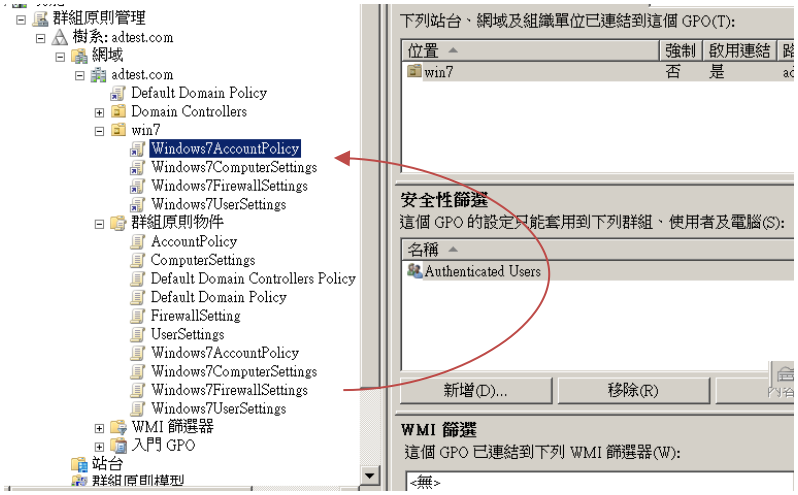


資料來源：本計畫整理

圖10 完成 GPO

二、套用說明

●將已完成匯入之 GPO，連結至欲部署之區域(如：網域(Domain)、組織單位(Organization Unit，以下簡稱 OU)等)，完成部署作業，詳見圖 11。

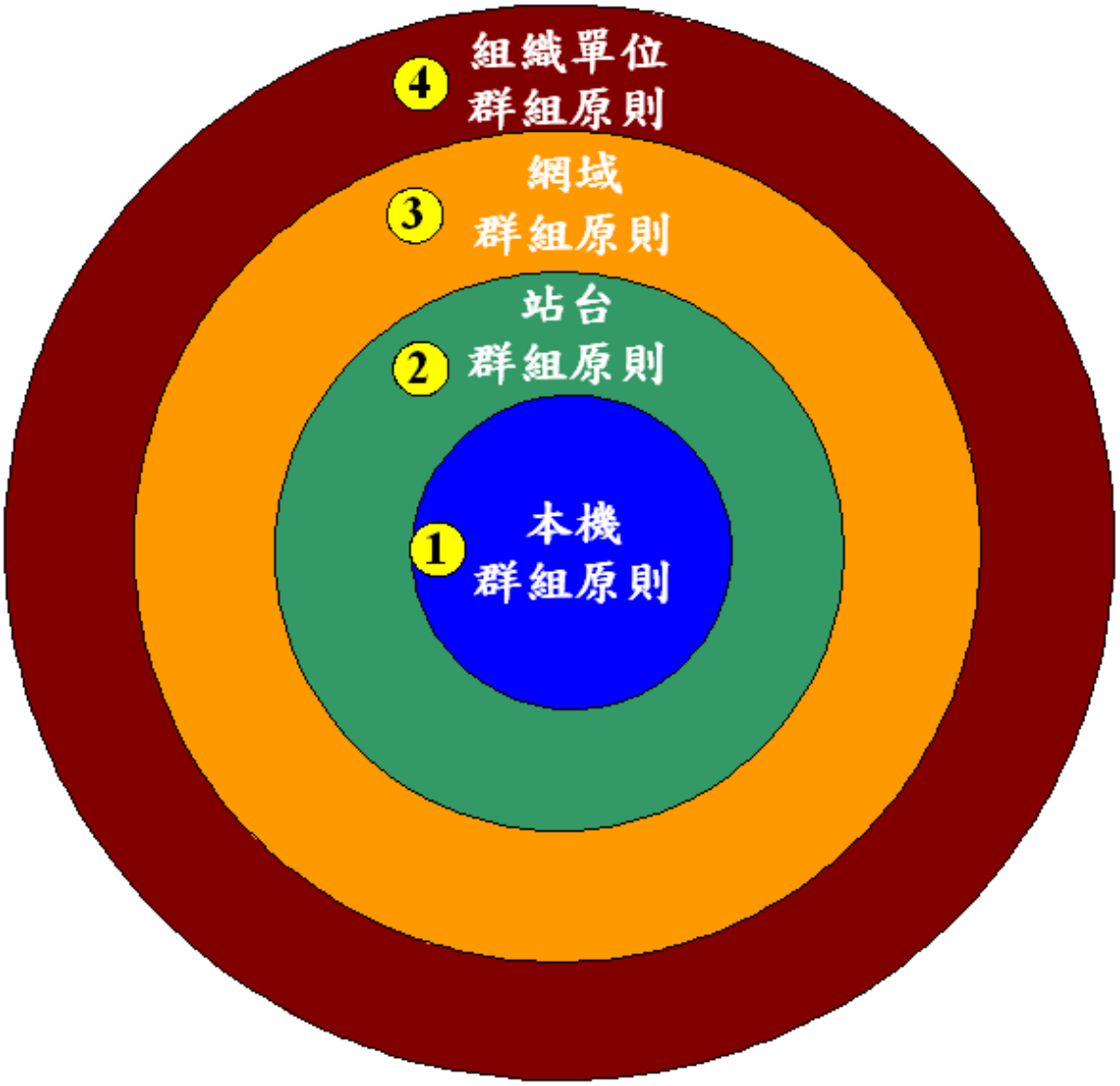


資料來源：本計畫整理

圖11 將 GPO 連結至 OU

三、套用順序

GPO 的順序會決定優先順序。順序是本機(Local)→站台(Site)→網域(Domain)→OU→子 OU。因此，子 OU 中之 GPO 的優先順序高於連結到父 OU 之 GPO 的優先順序；連結到父 OU 之 GPO 的優先順序高於連結到網域之 GPO 的優先順序；而連結到網域之 GPO 的優先順序高於連結到站台之 GPO 的優先順序。群組原則套用 GPO 的順序是由上而下，而且層級較高的設定會覆寫層級較低的設定，詳見圖 12。



資料來源：本計畫整理

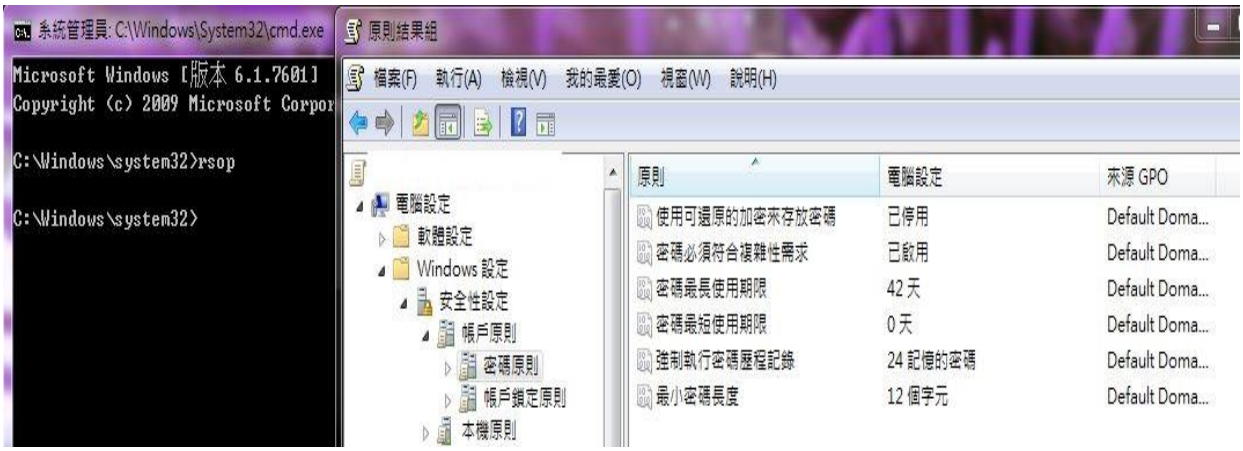
圖12 GPO 套用順序

四、原則檢視

在網域環境中，使用 RSOP 或 GPRESULT 來顯示原則結果組資訊，來檢視群組原則設定套用情形。

(一)使用 RSOP 檢視群組原則套用情形

以「系統管理員身分」執行「命令提示字元」，輸入「rsop」指令顯示原則結果組資訊，詳見圖 13。



資料來源：本計畫整理

圖13 使用 RSOP 指令顯示原則結果組資訊

(二)使用 GPRESULT 檢視群組原則套用情形

以「系統管理員身分」執行「命令提示字元」，輸入「gpresult /h <REPORT_NAME>.html」指令產出原則結果組資訊之 HTML 檔案。其中，<REPORT_NAME>參數可由使用者自行輸入欲命名之檔名，詳見圖 14。

資料來源：本計畫整理

圖14 使用 GPRESULT 指令產出原則結果組資訊之 HTML

五、恢復原始設定

在網域的環境中，可以透過 AD 伺服器移除 GPO 的設定值。在 AD 伺服器啟動群組原則管理後，先點選想要還原設定區域(如:OU 或網域)，此時會顯示該區域目前所套用的 GPO。接著選取要移除的 GPO 並點一下滑鼠右鍵，再點選「刪除」，即可將 GPO 的連結自區域中移除，待使用者電腦重新登入網域後，即可恢復原始設定。詳見圖 15。

資料來源：本計畫整理

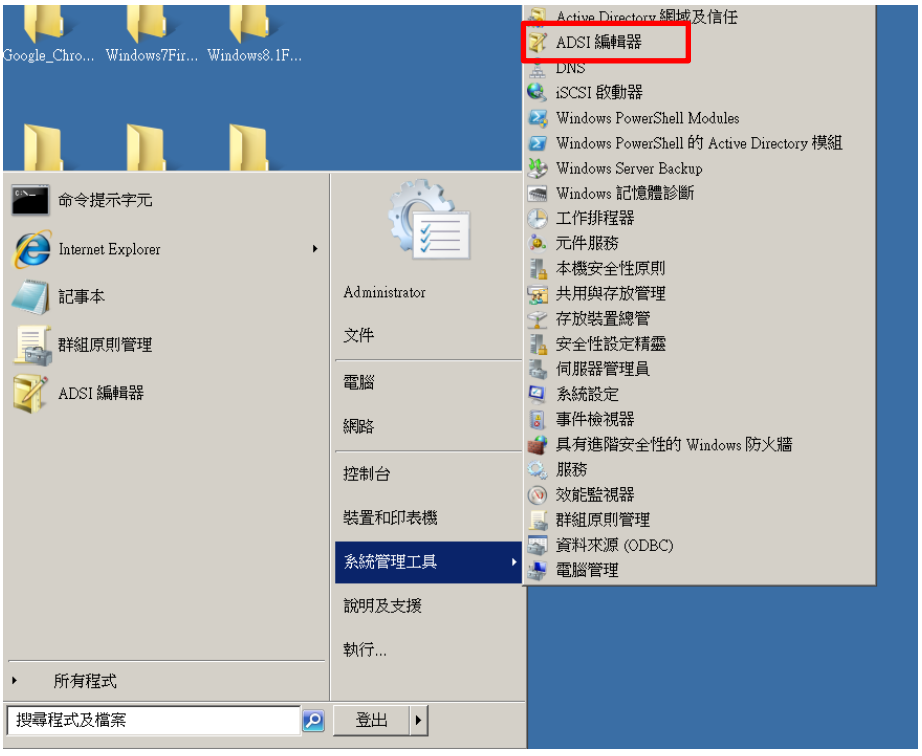
圖15 移除 GPO 之連結

參、 精細密碼原則

Windows Server 2003 以前的版本，AD 伺服器僅能針對網域設定單一帳戶原則(密碼原則與帳戶鎖定原則)，Windows Server 2008 之後的版本便提供精細密碼原則來解決此問題。其概念和群組原則物件(GPO)類似，透過容器與物件來設定，只是在精細密碼原則中是以「密碼設定容器(Password Settings Container，以下簡稱 PSC)」及「密碼設定物件(Password Settings Objects，以下簡稱 PSO)」來進行密碼原則設定與套用。

一、原則設定

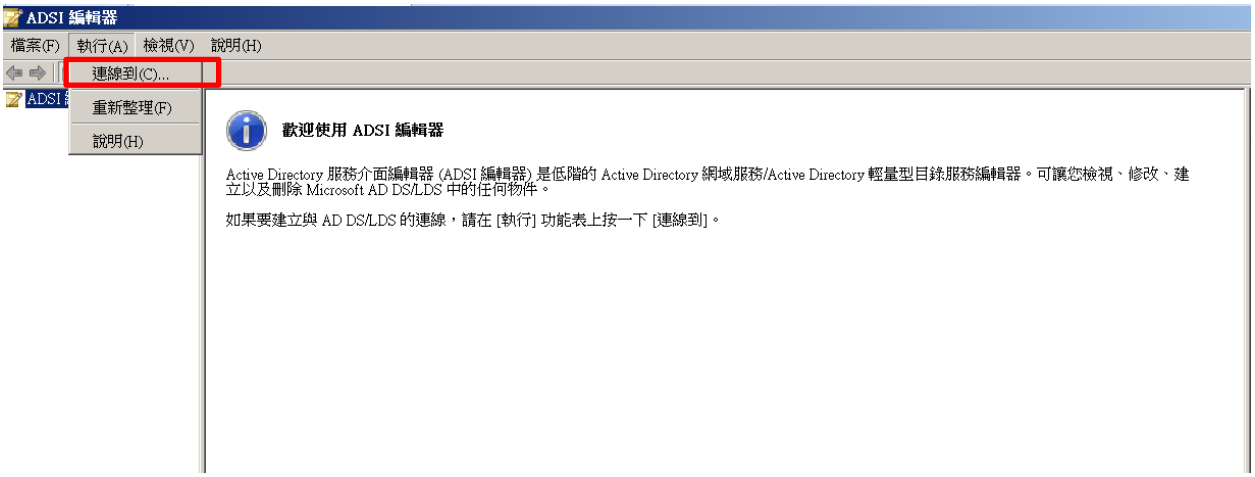
- 首先開啟「ADSI 編輯器」，「開始」→「系統管理工具」→「ADSI 編輯器」，詳見圖 16。



資料來源：本計畫整理

圖16 開啟 ADSI 編輯器

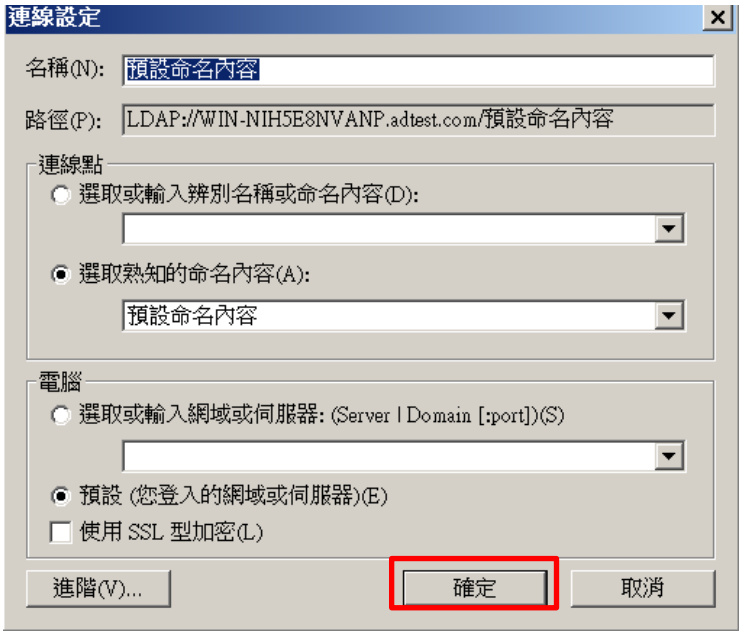
- 開啟 ADSI 編輯器後，點選「執行」→「連線到」，詳見圖 17。



資料來源：本計畫整理

圖17 建立與 AD DS/LDS 之連線

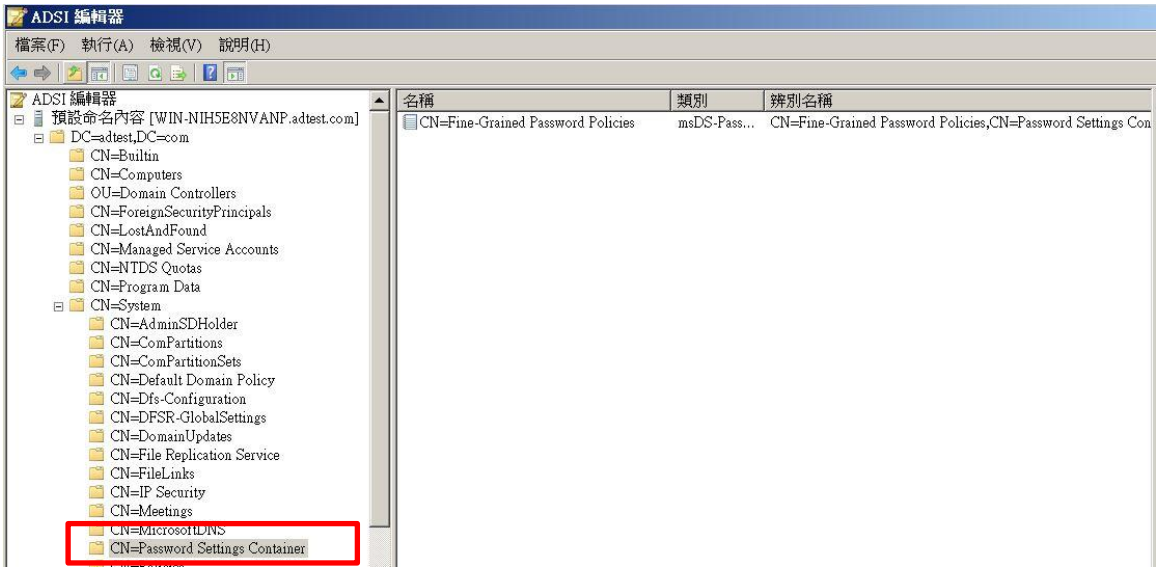
- 直接使用預設名稱直接點選「確定」，詳見圖 18



資料來源：本計畫整理

圖18 連線設定畫面

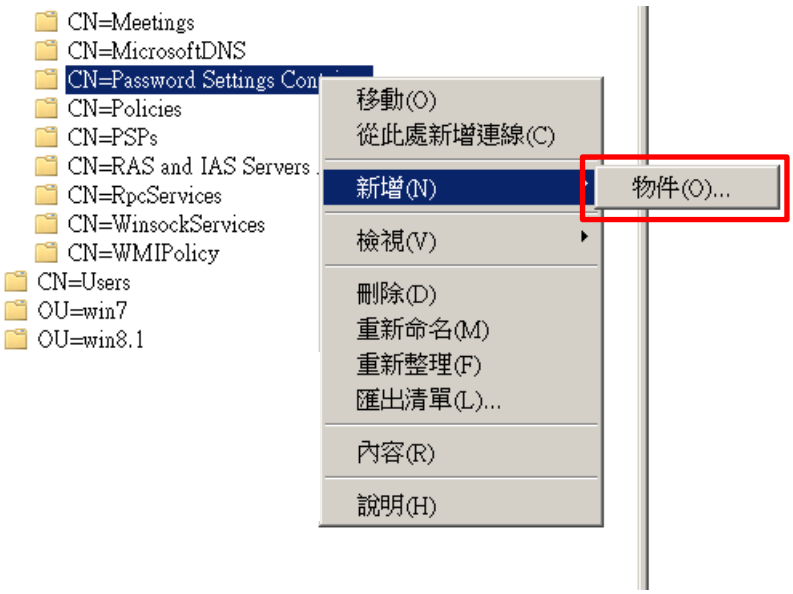
- 展開節點至「CN=Password Settings Container」，其路徑為：「預設命名內容」→「DC=domain name, DC=com」→「CN=System」→「CN=Password Settings Container」，詳見圖 19。



資料來源：本計畫整理

圖19 展開節點至「CN=Password Settings Container」

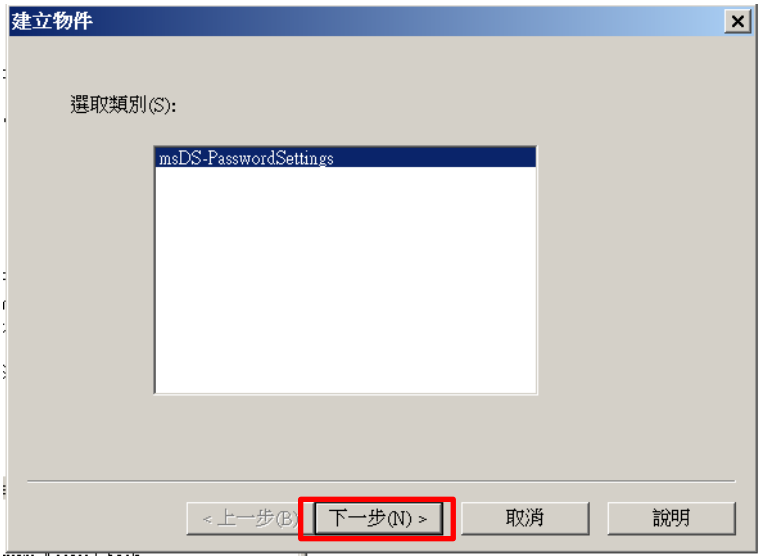
- 右鍵點選「CN=Password Settings Container」→「新增」→「物件」，詳見圖 20。



資料來源：本計畫整理

圖20 新增密碼原則物件

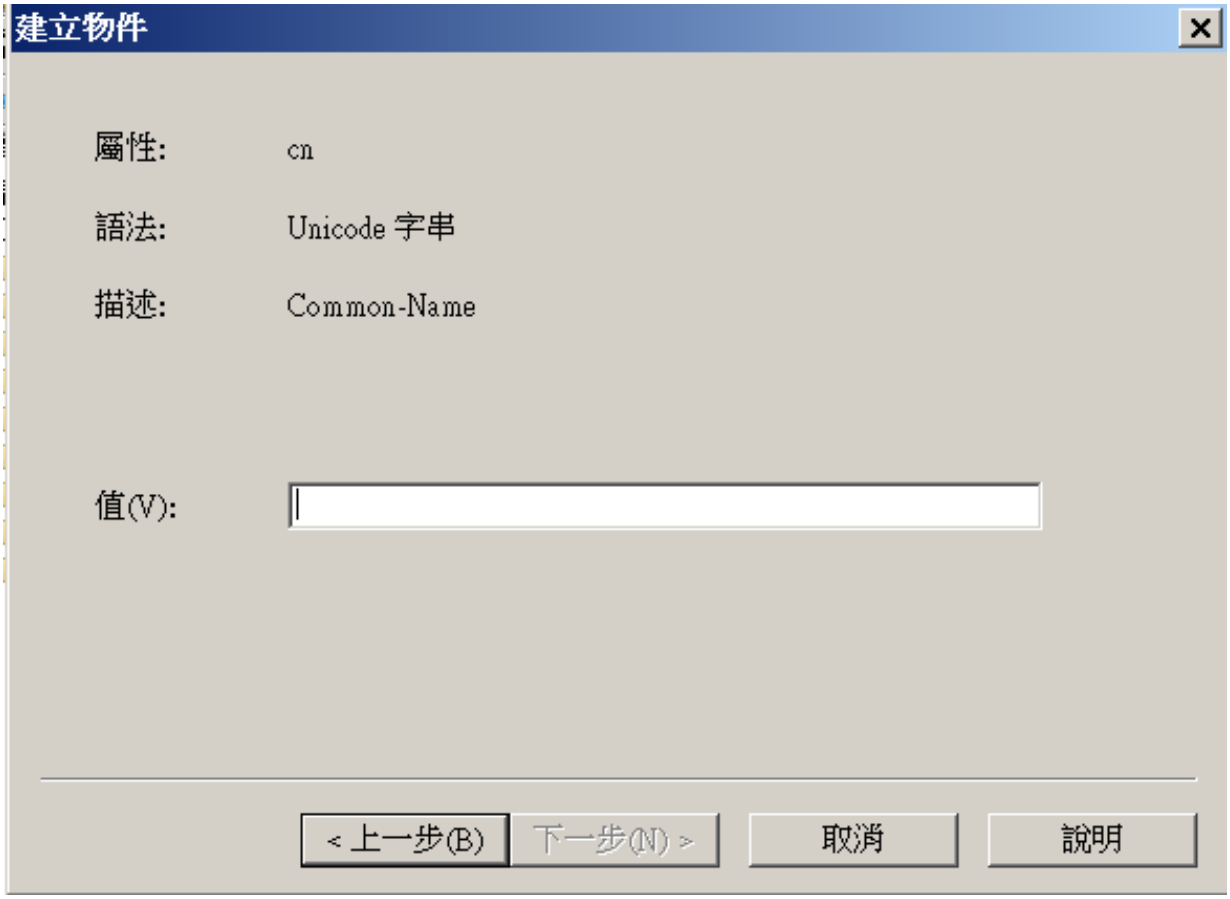
- 新增物件後，僅有「msDS-PasswordSettings」可選擇，點選「下一步」，詳見圖 21。



資料來源：本計畫整理

圖21 選擇「msDS-PasswordSettings」

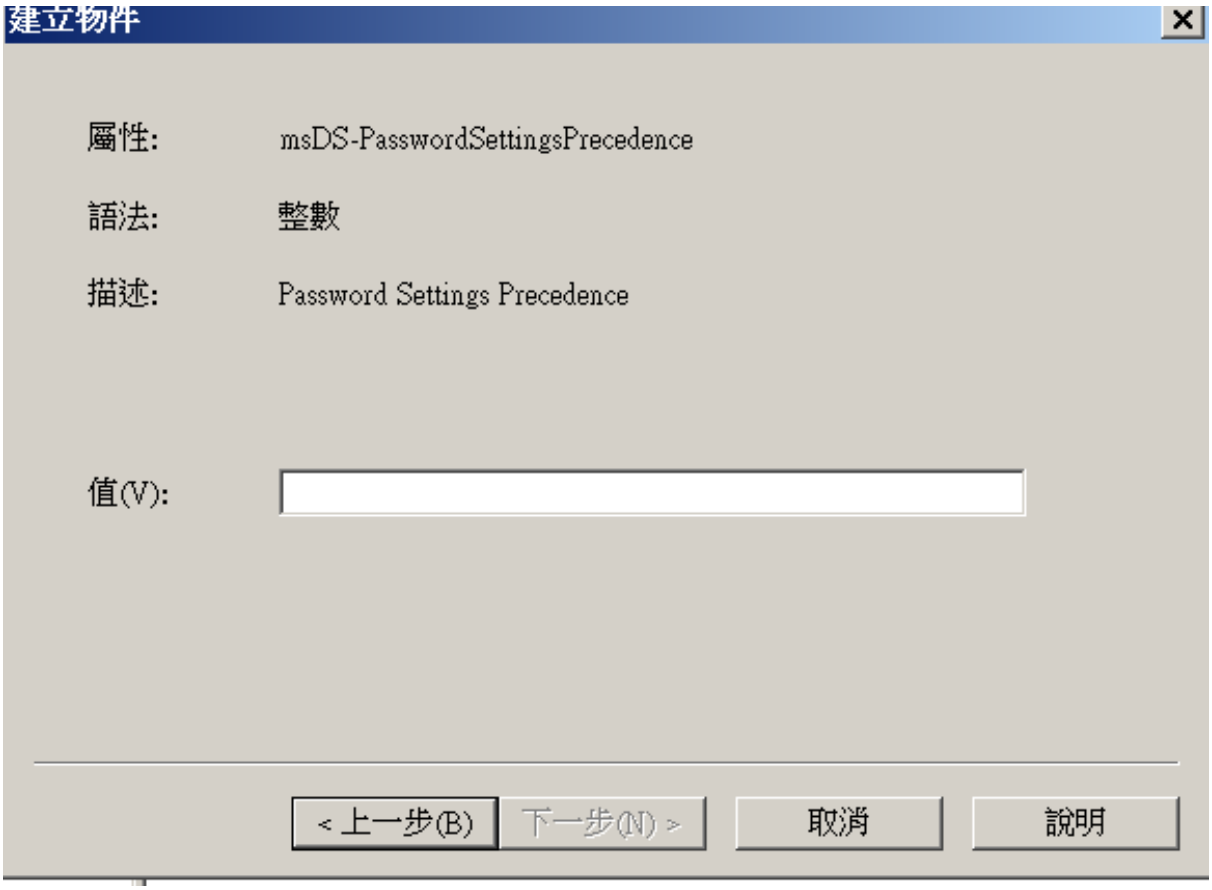
- 替密碼原則物件(PSO)進行命名，屬性「Common-Name」為密碼原則物件(PSO)之名稱，詳見圖 22。



資料來源：本計畫整理

圖22 設定屬性「Common-Name」

- 設定密碼原則物件(PSO)之優先權，需要輸入一個大於 1 的值。數值越小，優先權越大



資料來源：本計畫整理

圖23 設定屬性「msDS-PasswordSettingsPrecedence」

- 設定完成後，開始進行 9 項密碼原則設定。密碼原則設定與其對應之群組原則名稱詳見表 2。

表2　密碼原則設定與群組原則名稱對照表

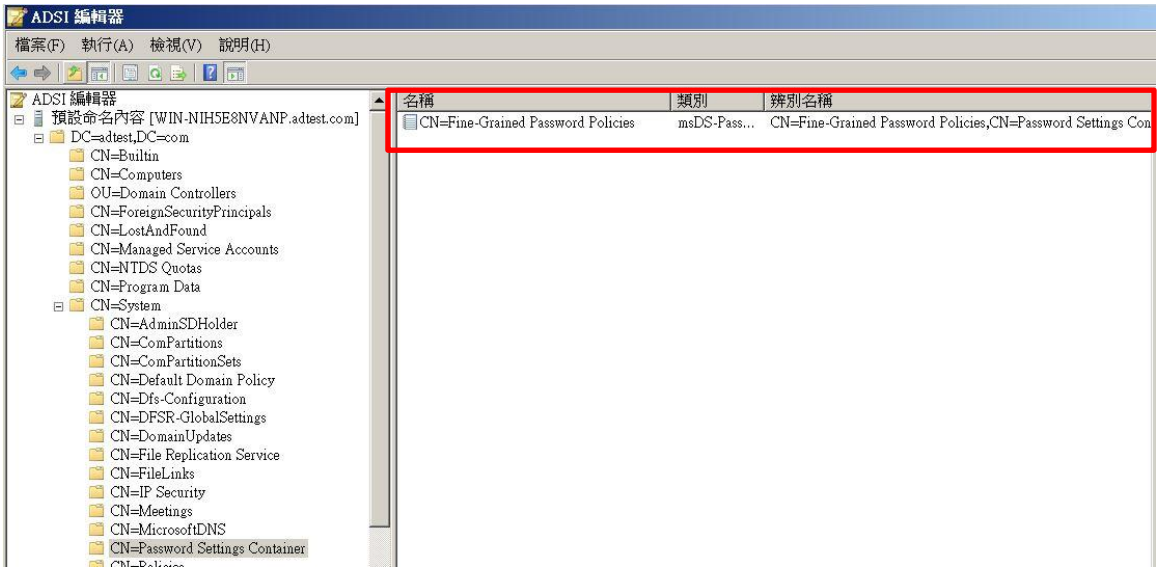
項次	密碼設定物件之密碼原則設定名稱	群組原則名稱	屬性格式
1	msDS-MinimumPasswordAge	密碼最短使用期限	dd:hh:mm:ss 如:1:00:00:00
2	msDS-MaximumPasswordAge	密碼最長使用期限	dd:hh:mm:ss 如:90:00:00:00

3	msDS-MinimumPasswordLength	最小密碼長度	0~255
4	msDS-PasswordComplexityEnabled	密碼必須符合複雜性需求	FALSE / TRUE
5	msDS-PasswordHistoryLength	強制執行密碼歷程記錄	0~1024
6	msDS-PasswordReversibleEncryptionEnabled	使用可還原的加密來存放密碼	FALSE / TRUE
7	msDS-LockoutThreshold	帳戶鎖定閾值	0~65535
8	msDS-LockoutObservationWindow	重設帳戶鎖定計數器的時間	dd:hh:mm:ss 如:00:01:30:00
9	msDS-LockoutDuration	帳戶鎖定期間	dd:hh:mm:ss 如:00:01:30:00

資料來源：本計畫整理

二、套用說明

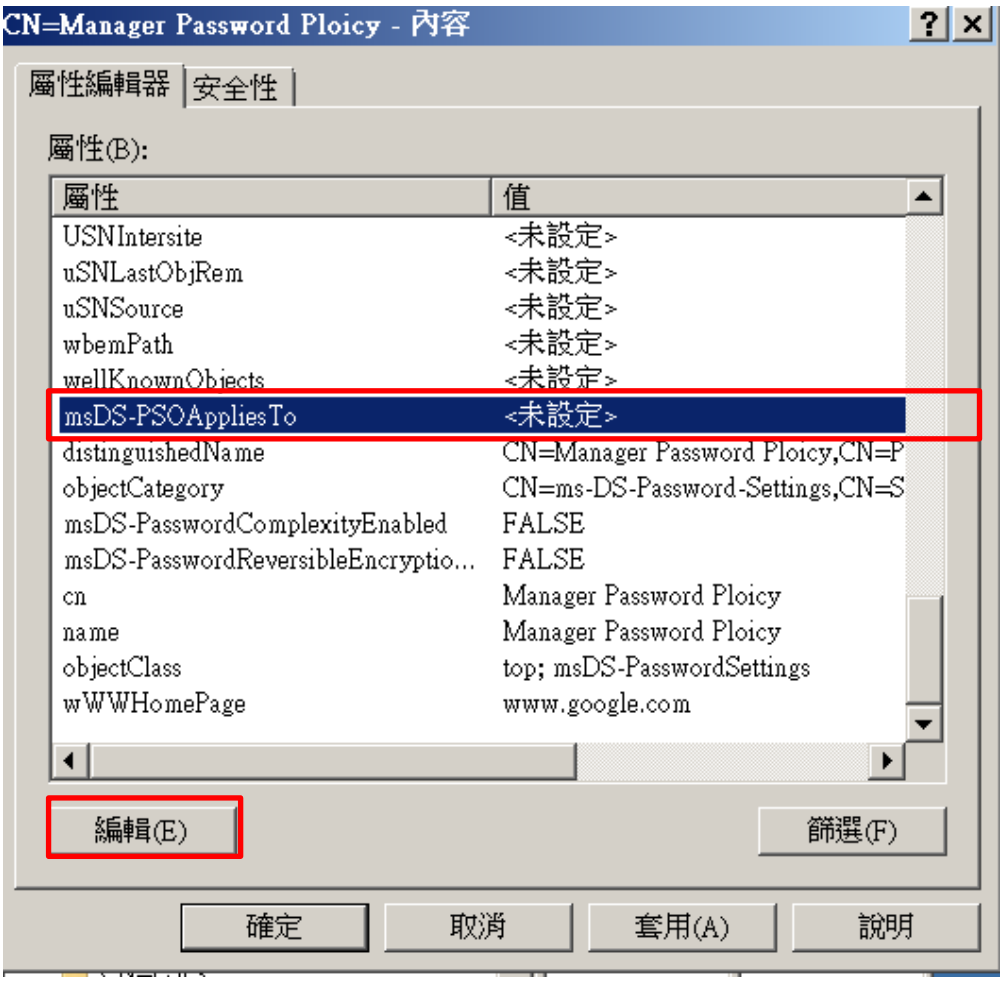
- 完成密碼原則物件(PSO)設定後，可在「ADSI 編輯器」右側視窗中，看到所建立之物件。選擇新增完成之密碼原則物件(PSO)，點選右鍵→「內容」，來設定套用之目標，詳見圖 24。



資料來源：本計畫整理

圖24 設定密碼原則物件(PSO)套用之目標

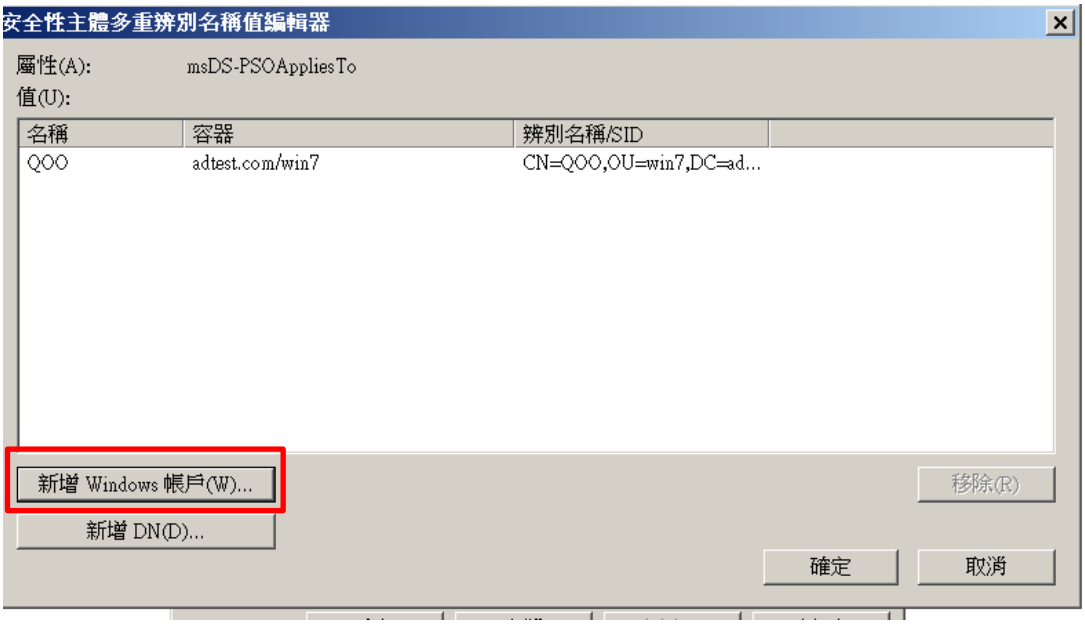
- 尋找屬性「msDS-PSOAppliesTO」，並點選「編輯」，詳見圖 25。



資料來源：本計畫整理

圖25 選擇屬性「msDS-PSOAppliesTO」

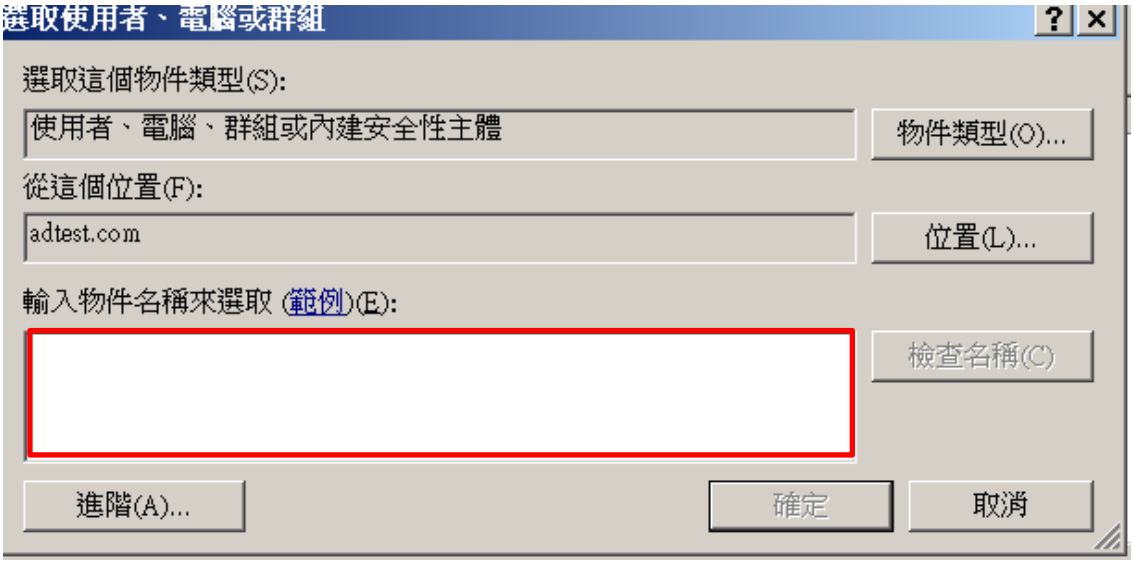
- 在編輯屬性「msDS-PSOAppliesTO」畫面中，點選「新增 Windows 帳戶」，詳見圖 26。



資料來源：本計畫整理

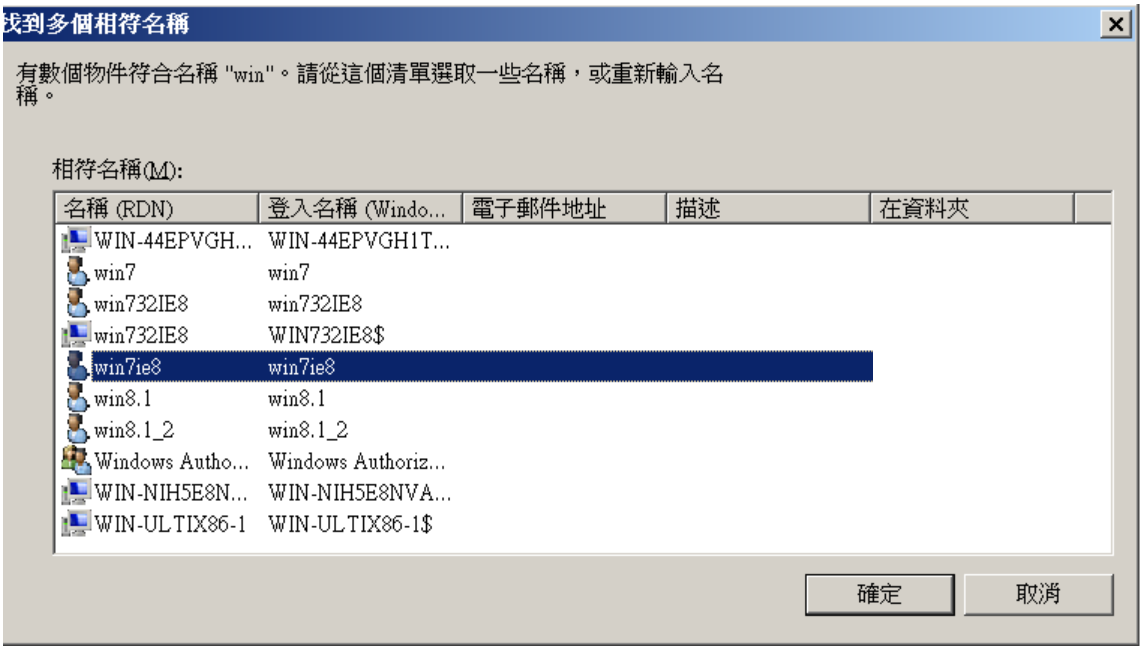
圖26 編輯屬性「msDS-PSOAppliesTO」

- 輸入欲套用該密碼原則物件(PSO)之使用者名稱，欲套用之使用者帳戶，詳見圖 27 與圖 28。



資料來源：本計畫整理

圖27 輸入欲套用之使用者名稱

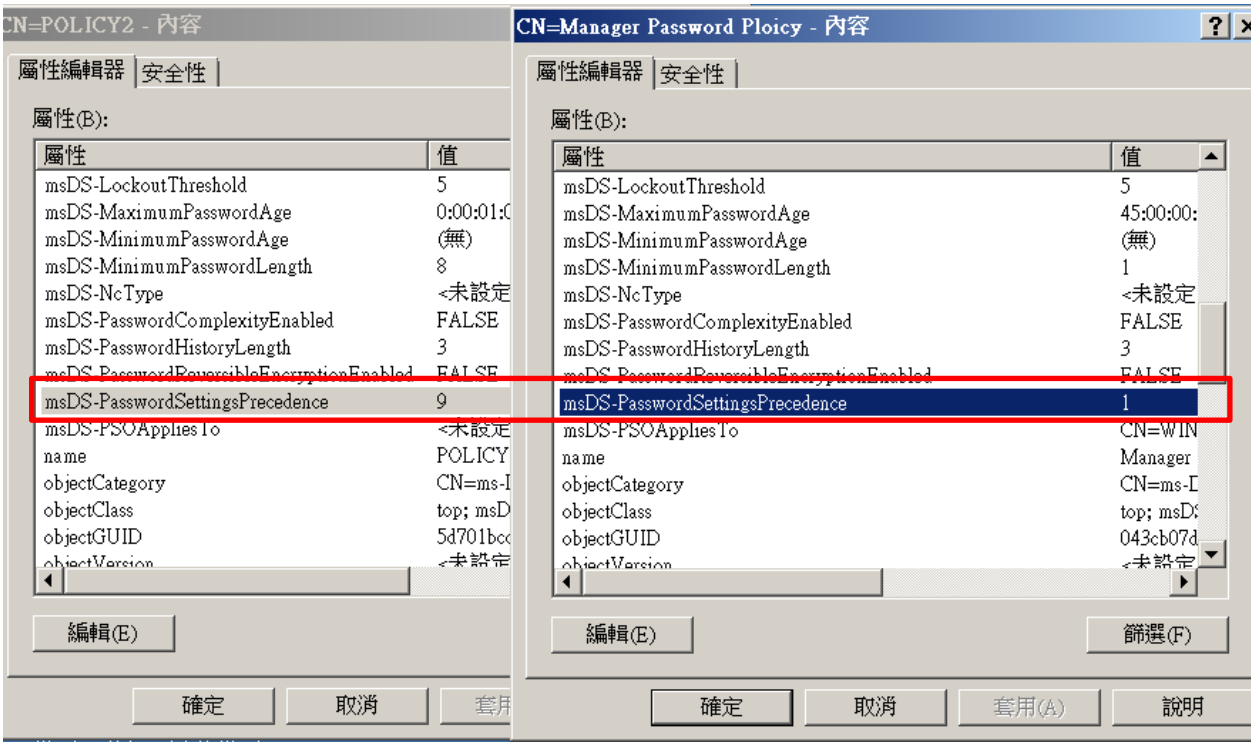


資料來源：本計畫整理

圖28 選擇欲套用之使用者帳戶

三、套用順序

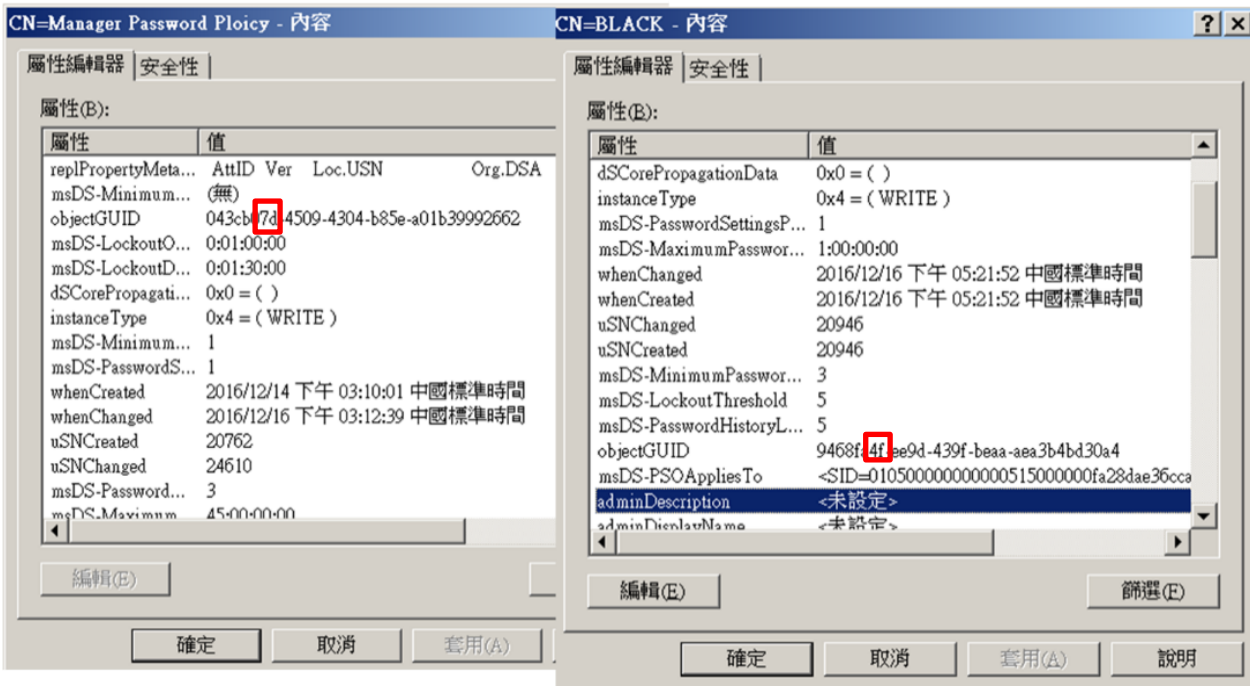
- 當 2 個密碼原則物件(PSO)套用到同一個使用者時，屬性「msDS-PasswordSettingsPrecedence」數值越小者，優先權越大。詳見圖 29。



資料來源：本計畫整理

圖29 密碼原則物件 PSO 套用優先權

- 當屬性「msDS-PasswordSettingsPrecedence」數值相同時，則以 Global Unique Identifier(以下簡稱 GUID)第一段之末兩碼來進行判斷。GUID 以 16 進位表示，數值越小代表優先權越大，詳見圖 30。



資料來源：本計畫整理

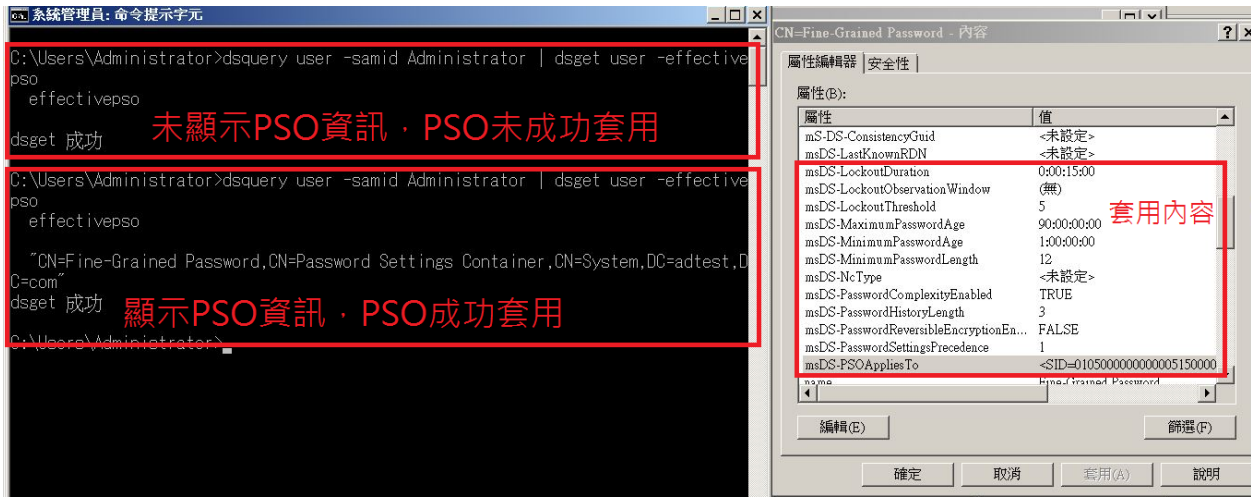
圖30 GUID 之比較

四、原則檢視

在網域環境中，使用 DSQUERY 指令或透過 ADSI 編輯器來檢視密碼設定物件套用情形。

(一)使用 DSQUERY 檢視精細密碼原則套用情形

- 以「系統管理員身分」開啟「命令提示字元」，輸入「dsquery user -samid <USERNAME> | dsget user -effectivepso」，檢視回傳結果之密碼原則物件名稱是否成功套用。其中，<USERNAME>參數可由使用者自行輸入使用者名稱。若成功顯示 PSO 之資訊，即代表 PSO 成功套用，；若僅顯示「dsget 成功」之訊息，即代表 PSO 未套用。詳見圖 31。

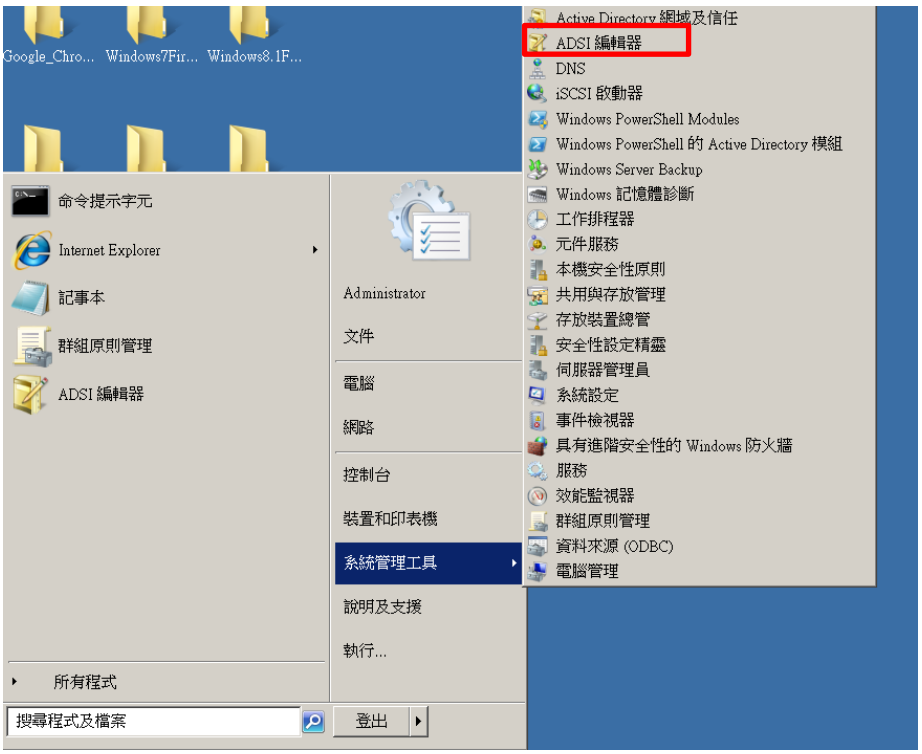


資料來源：本計畫整理

圖31 使用 DSQUERY 檢視密碼設定物件

(二)使用 ADSI 編輯器檢視精細密碼原則套用情形

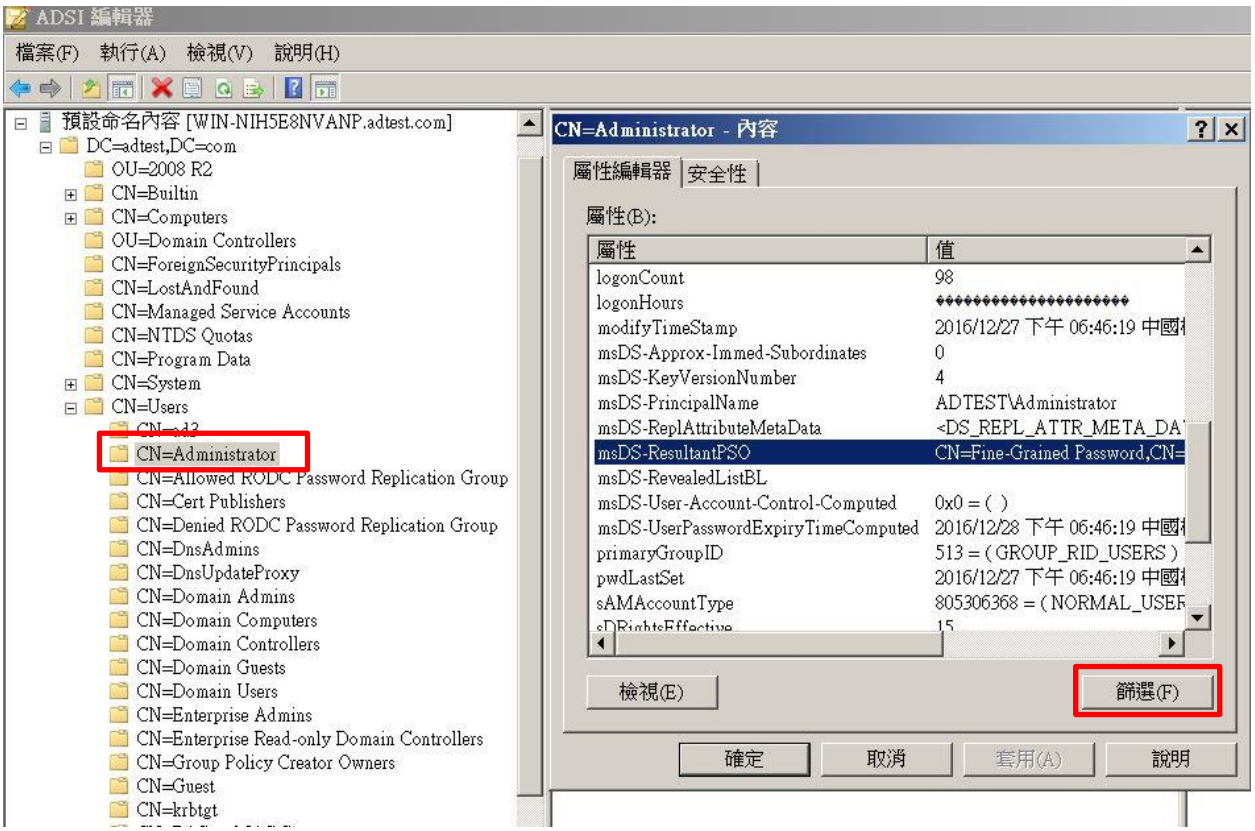
- 開啟「ADSI 編輯器」，「開始」→「系統管理工具」→「ADSI 編輯器」，詳見圖 32。



資料來源：本計畫整理

圖32 開啟 ADSI 編輯器

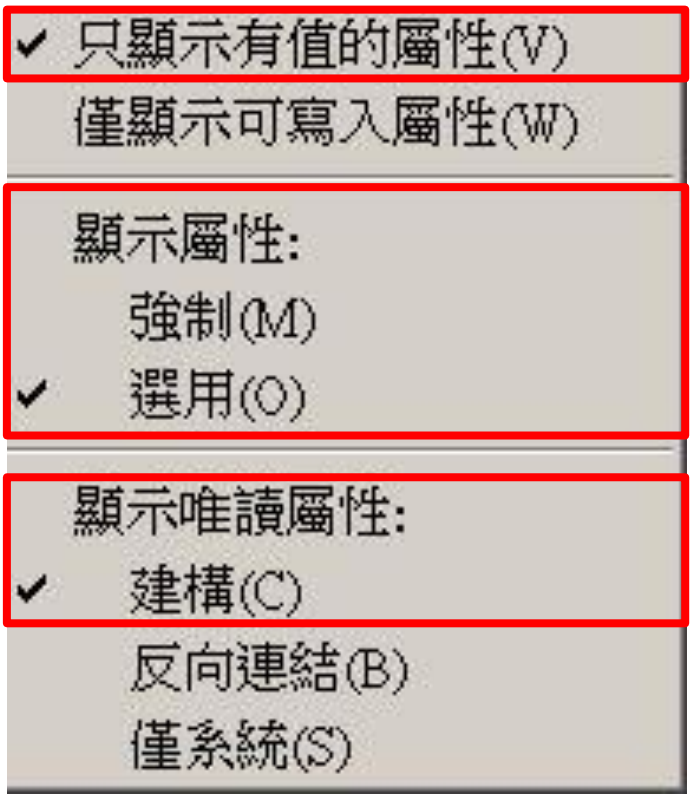
- 連線到預設命名內容，展開節點「DC=<Domain name>, DC=com」→「CN=User」，選擇欲檢視之使用者帳戶，點選右鍵→選擇「內容」，詳見圖 33。



資料來源：本計畫整理

圖33 檢視使用者之內容屬性

- 為快速尋找屬性「msDS-ResultantPSO」，可調整篩選配置。點擊「篩選」後，勾選「只顯示有值得的屬性」、「顯示屬性：選用」及「顯示唯獨屬性：建構」共 3 項篩選設定，詳見圖 34。



資料來源：本計畫整理

圖34 調整篩選配置設定

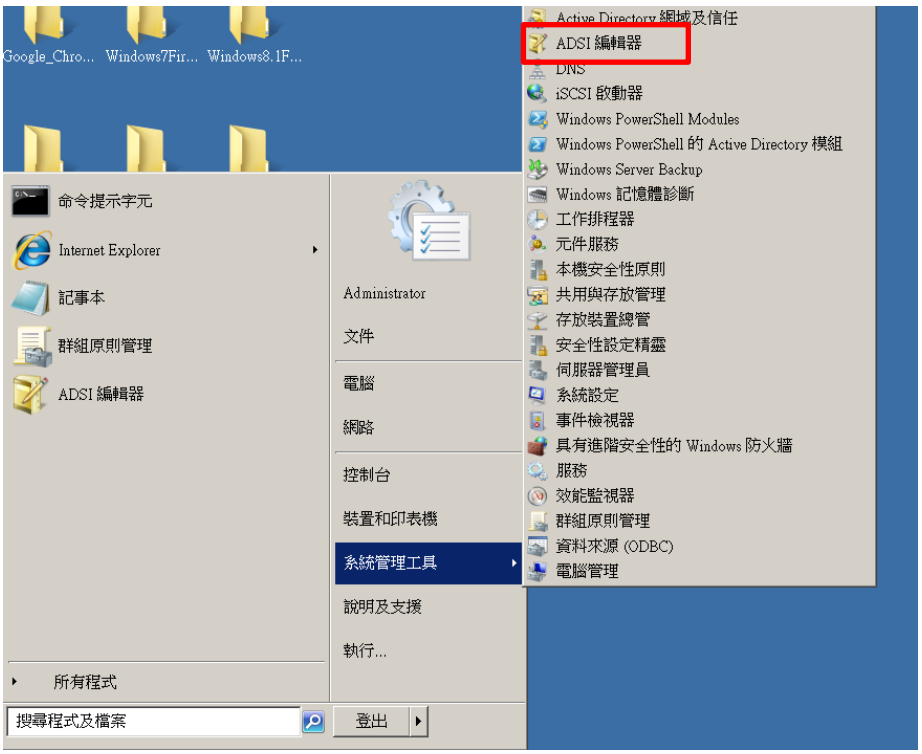
- 檢視屬性「msDS-ResultantPSO」之設定值，即可知 PSO 是否正確套用，詳見圖 35。

資料來源：本計畫整理

圖35 檢視屬性「msDS-ResultantPSO」

五、恢復原始設定

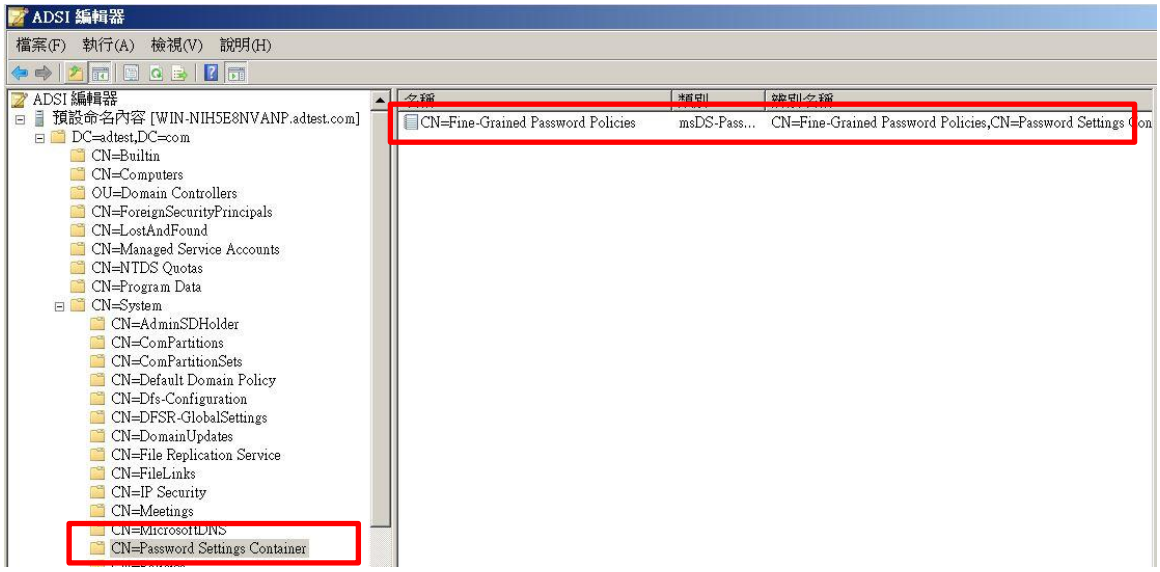
- 開啟「ADSI 編輯器」，「開始」→「系統管理工具」→「ADSI 編輯器」，詳見圖 36。



資料來源：本計畫整理

圖36 開啟 ADSI 編輯器

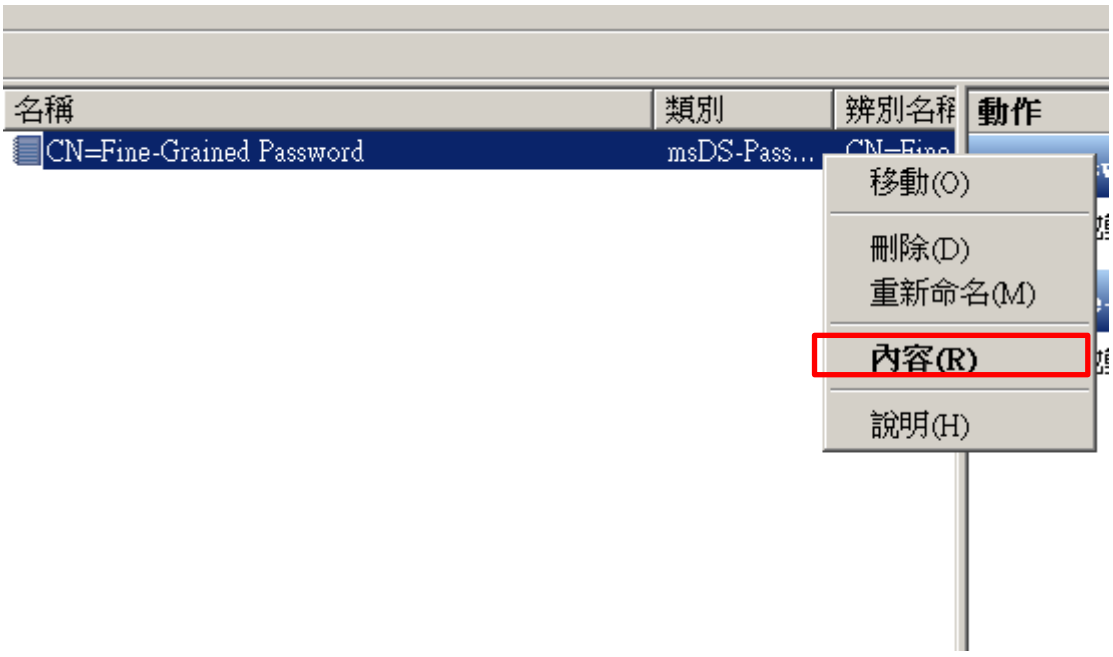
- 連線到預設命名內容，展開節點至「CN=Password Settings Container」，其路徑為：「預設命名內容→「DC=domain name, DC=com」→「CN=System」→「CN=Password Settings Container」，詳見圖 37。



資料來源：本計畫整理

圖37 展開節點至「CN=Password Settings Container」

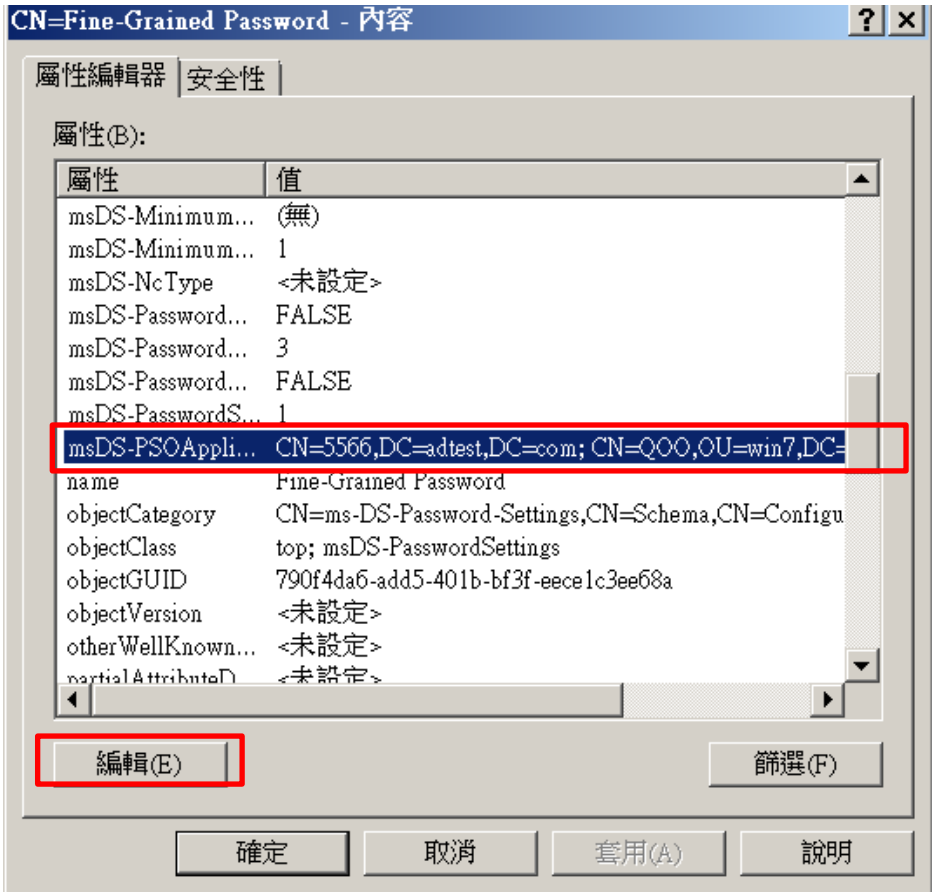
- 右鍵點選右側欄位的 PSO，點選「內容」，詳見圖 38。



資料來源：本計畫整理

圖38 編輯 PSO 內容

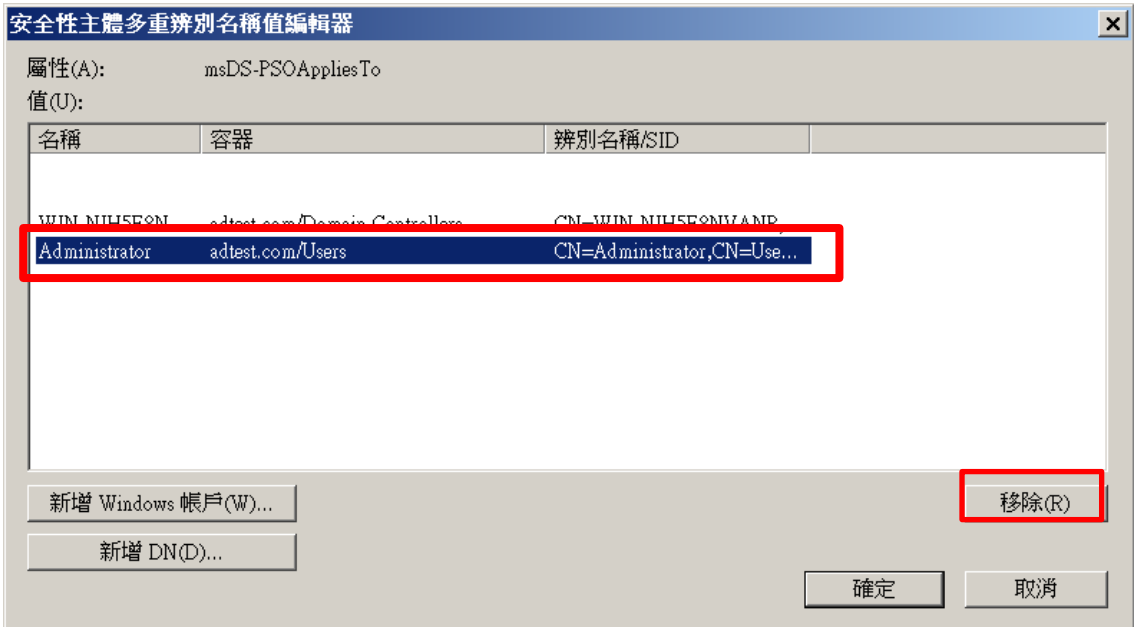
- 編輯屬性「msDS-PSOAppliesTO」，詳見圖 39。



資料來源：本計畫整理

圖39 編輯屬性「msDS-PSOAppliesTO」

- 選擇要移除的使用者帳戶，點選「移除」，即移除使用者與密碼原則物件之連結，待使用者電腦重新登入網域後，即可恢復原始設定。詳見圖 40



資料來源：本計畫整理

圖40 移除使用者名稱