

政府組態基準(GCB)實作研習活動 (Windows 7)

國家資通安全會報 技術服務中心



大綱

- 前言
- Windows 7政府組態基準項目分類
- Windows 7政府組態基準設定項目說明
- 問題與討論

- 目的

- 規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮

- 政府組態基準項目內容

- Windows 7

- Windows 7 Firewall

- Internet Explorer 8

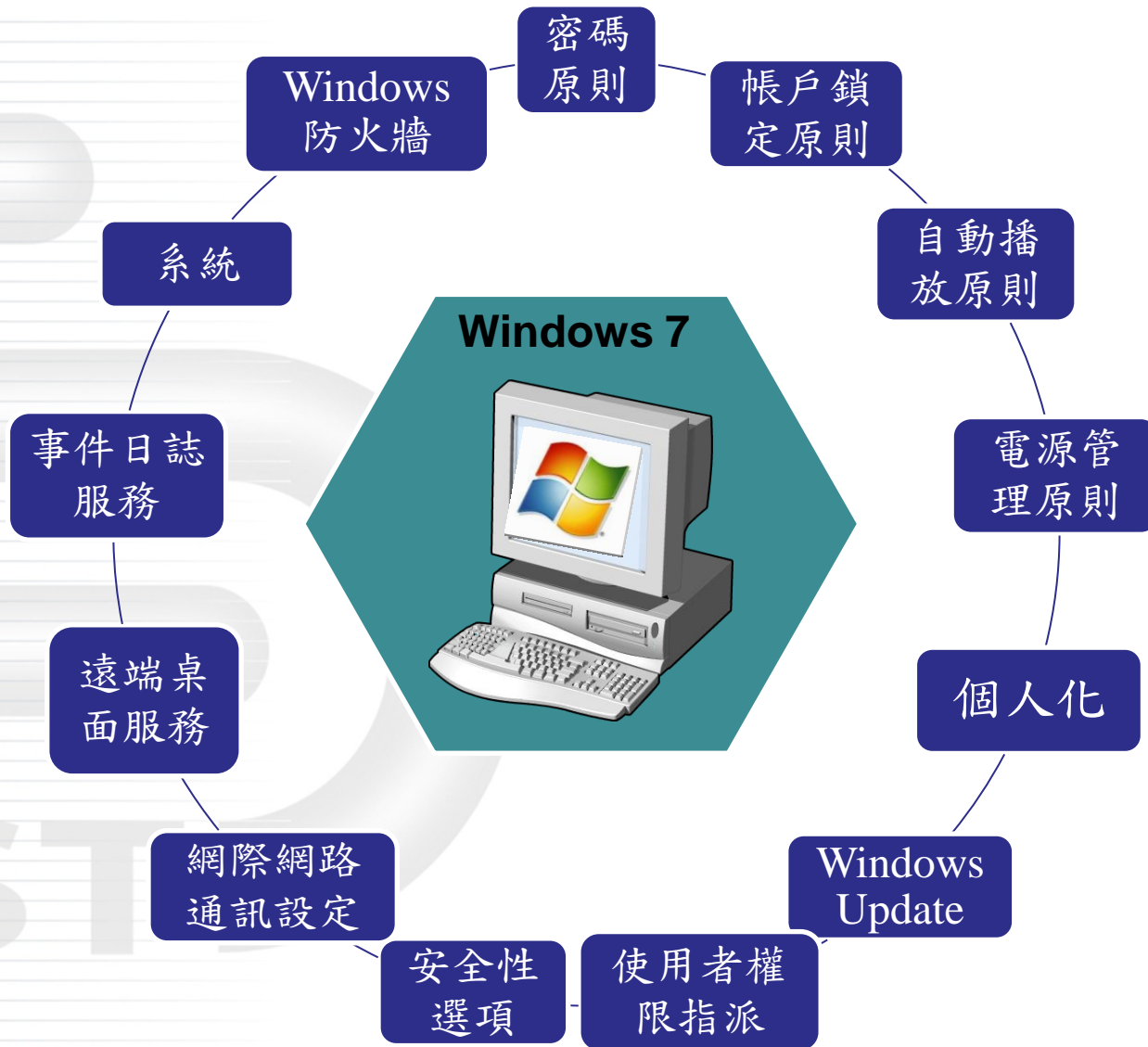


政府組態基準GCB項數統計

類別	項目名稱	項數統計
Windows 7	USGCB Account Policy	9
Windows 7	USGCB Windows 7 Computer Energy Policy	4
Windows 7	USGCB Windows 7 Computer Settings	225
Windows 7	USGCB Windows 7 User Settings	8
Windows 7 Firewall	USGCB Windows 7 Firewall Settings	35
Internet Explorer 8	USGCB Internet Explorer 8 Computer Settings	110
Internet Explorer 8	USGCB Internet Explorer 8 User Settings	5
總計		396

Windows 7政府組態基準 項目分類

Windows 7政府組態基準分類



Windows 7政府組態基準 設定項目說明



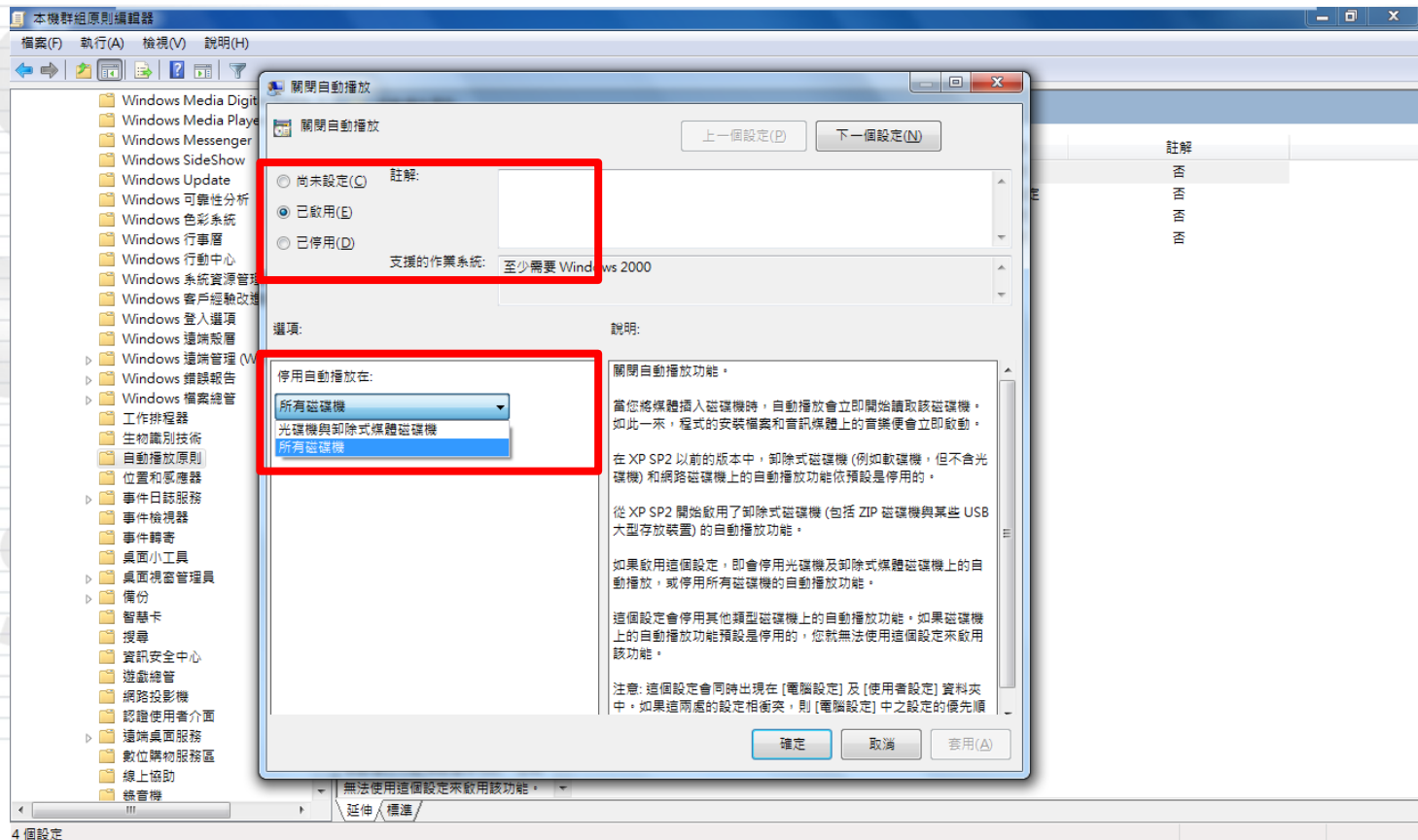
群組原則介紹

ICST

● 群組原則編輯器 (gpedit.msc)

— 啟用原則 / 停用原則 / 尚未設定

➤ 選項設定值



密碼原則

本機群組原則編輯器

檔案(F) 執行(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
 - 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
- 使用者設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本

原則	安全性設定
使用可還原的加密來存放密碼	已停用
密碼必須符合複雜性需求	已啟用
密碼最長使用期限	42 天
密碼最短使用期限	0 天
強制執行密碼歷程記錄	3 記憶的密碼
最小密碼長度	8 個字元



密碼最長使用期限

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
密碼最長使用期限

- 建議值

- 60(天)

- 說明

- 數值範圍：1~999 (天)

- 數值 0：代表密碼永遠不會到期



密碼最短使用期限

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
密碼最短使用期限

- 建議值

- 1(天)

- 說明

- 數值範圍：1~998 (天)

- 數值 0：代表立刻變更密碼

- 限制：密碼最短使用期限不得超過最長使用期限



密碼長度最小值

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
最小密碼長度

- 建議值

- 12個字元

- 說明

- 數值範圍

- 1~14(字元)

- 數值 0

- 代表不需密碼

密碼必須符合複雜性需求

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
密碼必須符合複雜性需求

- 建議值

- 啟用

- 說明

- 複雜性需求

- 不包含使用者帳戶名稱全名

- 長度至少為 6 個字元

- 包含英文大小寫字元、10 進位數字及非英文字母字元

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
強制執行密碼歷程記錄

- 建議值

- 24記憶的密碼

- 說明

- 設定新密碼或密碼更改時，不得與前24次之使用者密碼
相同

使用可還原的加密來存放密碼

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\
使用可還原的加密來存放密碼

- 建議值

- 停用

- 說明

- 使用可還原的加密來存放密碼，基本上和存放純文字密碼是相同的



帳戶鎖定原則

ICST

本機群組原則編輯器

檔案(F) 執行(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
 - 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
- 使用者設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本

原則	安全性設定
重設帳戶鎖定計數器的時間間隔	30 分鐘
帳戶鎖定時間	30 分鐘
帳戶鎖定閾值	5 次不正確的登入嘗試



帳戶鎖定閾值

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾(口`)值

- 建議值

- 5次不正確的登入嘗試

- 說明

- 數值範圍

- 0~999(次)

- 數值 0

- 永不鎖定帳戶

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定時間

- 建議值

- 15分鐘

- 說明

- 數值範圍

- 0~99999(分鐘)

- 限制

- 已設定帳戶鎖定閾值時，此原則設定才有意義

- 已定義帳戶鎖定閾值，帳戶鎖定期間必須大於或等於重設時間

重設帳戶鎖定計數器的時間

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\重設帳戶鎖定計數器的時間間隔

- 建議值

- 15分鐘

- 說明

- 數值範圍

- 1~99999(分鐘)

- 限制

- 指定帳戶鎖定閾值時，此原則設定才有意義

- 已定義帳戶鎖定閾值，此重設時間必須小於或等於帳戶鎖定期間

自動播放原則

自動播放原則

本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

← → [Icons]

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - Windows 元件
 - ActiveX Installer 服務
 - BitLocker 磁碟機加密
 - HomeGroup
 - Internet Explorer
 - Internet Information Services
 - NetMeeting
 - Parental Controls
 - RSS 摘要
 - Tablet PC
 - Windows Anytime Upgrade
 - Windows Defender
 - Windows Installer
 - Windows Mail
 - Windows Media Center
 - Windows Media Digital Rights Me
 - Windows Media Player
 - Windows Messenger
 - Windows SideShow
 - Windows Update
 - Windows 可靠性分析
 - Windows 色彩系統
 - Windows 行事曆
 - Windows 行動中心
 - Windows 系統資源管理員
 - Windows 客戶經驗改進計畫
 - Windows 登入選項
 - Windows 遠端殼層
 - Windows 遠端管理 (WinRM)
 - Windows 錯誤報告
 - Windows 檔案總管
 - 工作排程器
 - 生物識別技術**
 - 自動播放原則**
 - 位置感應器
 - Windows 遠端管理 (WinRM)
 - Windows 錯誤報告
 - Windows 檔案總管
 - 工作排程器
 - 生物識別技術
 - 自動播放原則
 - 位置感應器
 - 事件日誌服務

自動播放原則

選取一個項目來檢視它的描述。

設定	狀態
<input checked="" type="checkbox"/> 關閉自動播放	啟用
<input checked="" type="checkbox"/> 請勿設定 [一律進行此動作] 核取方塊	啟用
<input checked="" type="checkbox"/> 關閉非磁碟區裝置的自動播放	啟用
<input checked="" type="checkbox"/> AutoRun 的預設行為	啟用

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\自動播放原則
 \AutoRun的預設行為

- 建議值

- 啟用

- 不執行任何Autorun命令

- 說明

- AutoRun 命令一般儲存於 autorun.inf 檔案中。它們通常會啟動安裝程式或其他程式

- 啟用此原則，並選擇 [不執行任何Autorun命令]

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\自動播放原則\關閉自動播放

- 建議值

- 啟用

- 停用所有磁碟機

- 說明

- 啟用這個原則，就不會為磁碟區裝置(如：軟碟、硬碟、外接式硬碟、USB快閃式硬碟、光碟機等)啟用自動播放

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\自動播放原則\關閉非磁碟區裝置的自動播放

- 建議值

- 啟用

- 說明

- 啟用這個原則，就不會為非磁碟區裝置(如：數位相機、行動裝置等)啟用自動播放

電源管理原則

本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - Windows 元件
 - 印表機
 - 系統
 - iSCSI
 - Kerberos
 - Windows HotStart
 - Windows 時間服務
 - Windows 檔案保護
 - 分散式 COM
 - 可信賴平台模組服務
 - 地區設定服務
 - 系統還原
 - 使用者設定檔
 - 卸除式儲存裝置存取權
 - 指令碼
 - 效能控制台
 - 復原
 - 登入
 - 群組原則
 - 裝置安裝
 - 裝置重新導向
 - 資料重新導向
 - 電源管理**
 - 按鈕設定
 - 通知設定值
 - 硬體設定
 - 視訊與顯示設定
 - 睡眠設定

電源管理

選取一個項目來檢視它的描述：

設定	狀態	註解
按鈕設定		
通知設定值		
硬體設定		
視訊與顯示設定		
睡眠設定		
指定自訂使用中電源計劃	尚未設定	否
選取使用中電源計劃	尚未設定	否

關閉顯示器(使用電池)

- 設定路徑

- 電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定
\關閉顯示器(使用電池)

- 建議值

- 啟用

- 1200(秒)(即 20分鐘)

- 說明

- 啟用原則，並指定 Windows 關閉顯示器前的閒置時間

- 經過指定時間之後，Windows 便會關閉顯示器

關閉顯示器(使用一般電源)

- 設定路徑

- 電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定
\關閉顯示器(使用一般電源)

- 建議值

- 啟用

- 1200(秒)(即 20分鐘)

- 說明

- 啟用原則，並指定 Windows 關閉顯示器前的閒置時間

- 經過指定時間之後，Windows 便會關閉顯示器

指定系統休眠逾時(使用電池)

- 設定路徑

- 電腦設定\系統範本設定\系統\電源管理\睡眠設定\指定系統休眠逾時(使用電池)

- 建議值

- 啟用

- 3600(秒)(即 60分鐘)

- 說明

- 啟用原則，並指定 Windows 將系統轉換為休眠之前的閒置時間

- 經過指定時間之後，Windows 便會進入休眠狀態



指定系統休眠逾時(使用一般電源)

- 設定路徑

- 電腦設定\系統範本設定\系統\電源管理\睡眠設定\指定系統休眠逾時(使用一般電源)

- 建議值

- 啟用

- 3600(秒)(即 60分鐘)

- 說明

- 啟用原則，並指定 Windows 將系統轉換為休眠之前的閒置時間

- 經過指定時間之後，Windows 便會進入休眠狀態



喚醒電腦時必須使用密碼(使用電池)

- 設定路徑

- 電腦設定\系統管理範本\系統\電源管理\睡眠設定\喚醒電腦時必須使用密碼(使用電池)

- 建議值

- 啟用

- 說明

- 系統從休眠狀態中重新啟動時，必須輸入使用者密碼



喚醒電腦時必須使用密碼(使用一般電源)

- 設定路徑

- 電腦設定\系統管理範本\系統\電源管理\睡眠設定\喚醒電腦時必須使用密碼(使用一般電源)

- 建議值

- 啟用

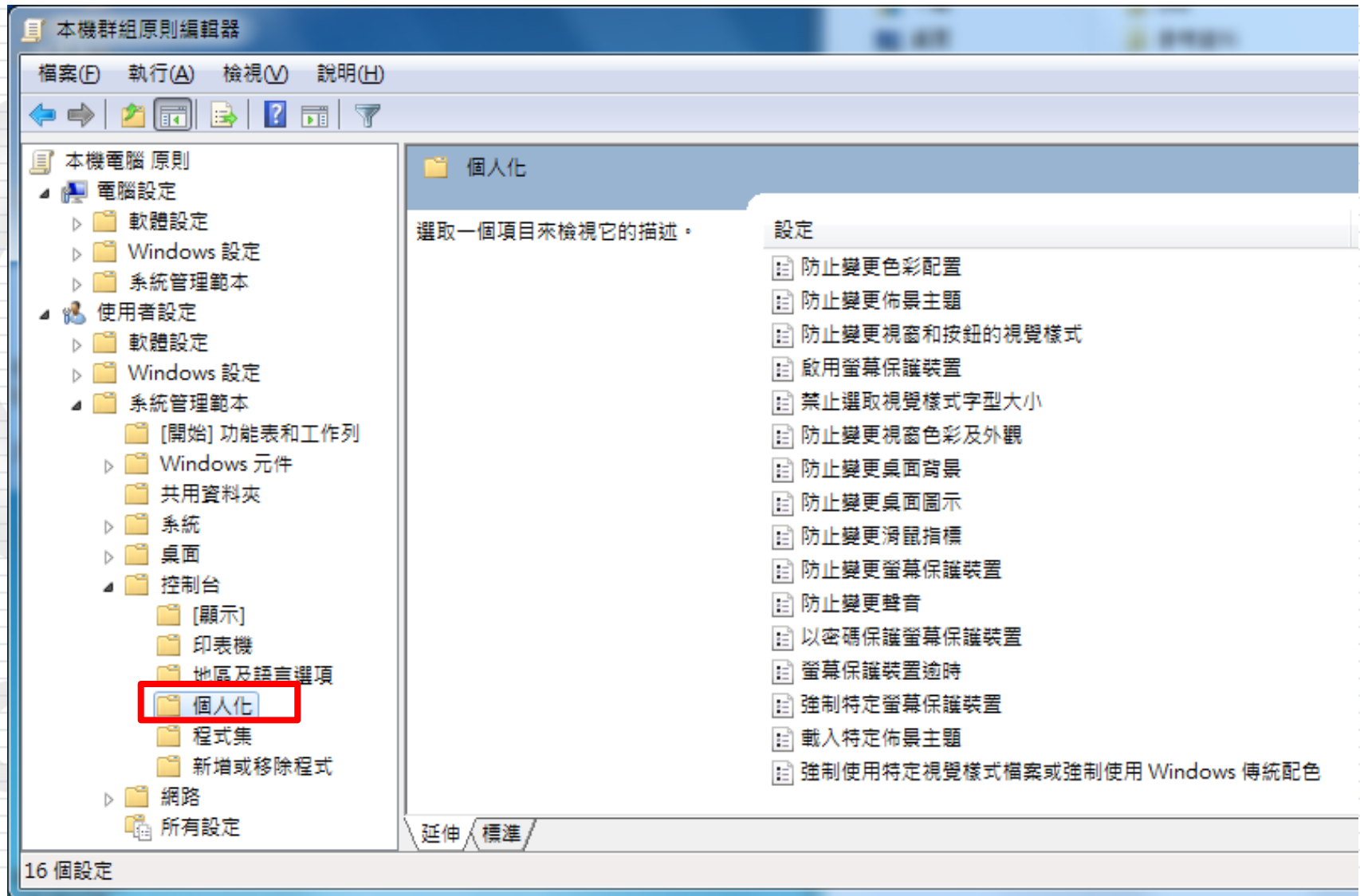
- 說明

- 系統從休眠狀態中重新啟動時，必須輸入使用者密碼



個人化





本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
- 使用者設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - [開始] 功能表和工作列
 - Windows 元件
 - 共用資料夾
 - 系統
 - 桌面
 - 控制台
 - [顯示]
 - 印表機
 - 地區及語言選項
 - 個人化**
 - 程式集
 - 新增或移除程式
 - 網路
 - 所有設定

個人化

選取一個項目來檢視它的描述。

設定

- 防止變更色彩配置
- 防止變更佈景主題
- 防止變更視窗和按鈕的視覺樣式
- 啟用螢幕保護裝置
- 禁止選取視覺樣式字型大小
- 防止變更視窗色彩及外觀
- 防止變更桌面背景
- 防止變更桌面圖示
- 防止變更滑鼠指標
- 防止變更螢幕保護裝置
- 防止變更聲音
- 以密碼保護螢幕保護裝置
- 螢幕保護裝置逾時
- 強制特定螢幕保護裝置
- 載入特定佈景主題
- 強制使用特定視覺樣式檔案或強制使用 Windows 傳統配色

16 個設定

延伸 標準

- 設定路徑

- 使用者設定\系統管理範本\控制台\個人化\啟用螢幕保護裝置

- 建議值

- 啟用

- 說明

- 啟用此原則，下列條件需成立，螢幕保護裝置才會執行

- 已透過設定或 [控制台] 將螢幕保護裝置逾時設定為非零的值

● 設定圖示



- 設定路徑

- 使用者設定\系統管理範本\控制台\個人化\螢幕保護裝置逾時

- 建議值

- 啟用

- 900秒 (即15分鐘)

- 說明

- 啟用原則，需指定使用者閒置時間經過多久後，啟動螢幕保護裝置

- 閒置時間可以設定在最少 1 秒到最多 86,400 秒 (或 24 小時) 之間

- 設為零，螢幕保護裝置將不會啟動

- 設定路徑

- 使用者設定\系統管理範本\控制台\個人化\以密碼保護螢幕保護裝置

- 建議值

- 啟用

- 說明

- 啟用原則，所有螢幕保護裝置都會受到密碼保護

- 解除螢幕保護裝置時，需輸入使用者密碼以進行解鎖



Windows Update

ICST

本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - Windows 元件
 - ActiveX Installer 服務
 - BitLocker 磁碟機加密
 - HomeGroup
 - Internet Explorer
 - Internet Information Services
 - NetMeeting
 - Parental Controls
 - RSS 摘要
 - Tablet PC
 - Windows Anytime Upgrade
 - Windows Defender
 - Windows Installer
 - Windows Mail
 - Windows Media Center
 - Windows Media Digital Rights Ma
 - Windows Media Player
 - Windows Messenger
 - Windows SideShow
 - Windows Update

Windows Update

選取一個項目來檢視它的描述。

設定	狀態
不要在 [關閉 Windows] 對話方塊中顯示 [安裝更新並關機] ...	尚未設定
不要將 [關閉 Windows] 對話方塊中的預設選項調整為 [安裝...	尚未設定
啟用 Windows Update 電源管理以自動喚醒系統安裝排程...	尚未設定
設定自動更新	尚未設定
指定近端內部網路 Microsoft 更新服務的位置	尚未設定
自動更新偵測頻率	尚未設定
允許非系統管理員收到更新通知	尚未設定
開啟軟體通知	尚未設定
允許立即安裝自動更新	尚未設定
透過自動更新安裝建議的更新	尚未設定
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	尚未設定
再次提示排程安裝所需的重新啟動	尚未設定
延遲排程安裝的重新啟動	尚未設定
重新排程已經排程好的自動更新安裝	尚未設定
啟用用戶端目標鎖定	尚未設定
允許來自內部網路 Microsoft 更新服務位置的已簽署更新	尚未設定

16 個設定

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows Update\
設定自動更新

- 建議值

- 啟用

- 3-自動下載和通知我安裝

- 說明

- 啟用原則，將會設定Windows自動更新與通知

- 設定值為 [自動下載和通知我安裝]



重新排程已經排程好的自動更新 安裝

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows Update\
重新排程已經排程好的自動更新安裝

- 建議值

- 啟用

- 1分鐘

- 說明

- 設成啟用，之前 [尚未發生的已排程安裝]，將於電腦下次啟動後，在指定的分鐘數後繼續開始

- 停用 [設定自動更新] 原則，此原則就無效



使用者權限指派

ICST

本機群組原則編輯器

檔案(F) 執行(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 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
- 使用者設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本

原則	安全性設定
允許本機登入	_vmware__Guest,Adm...
允許透過遠端桌面服務登入	Administrators,Remote...
以批次工作登入	Administrators,Backup ...
以服務方式登入	NT SERVICE\ALL SERVI...
同步處理目錄服務資料	
在驗證後模擬用戶端	LOCAL SERVICE,NETW...
存取認證管理員做為信任的呼叫者	
取代處理程序等級權杖	LOCAL SERVICE,NETW...
取得檔案或其他物件的擁有權	Administrators
拒絕以批次工作登入	
拒絕以服務方式登入	
拒絕本機登入	Guest
拒絕從網路存取這台電腦	
拒絕透過遠端桌面服務登入	
建立分頁檔	Administrators
建立永久共用物件	
建立符號連結	Administrators
建立通用物件	LOCAL SERVICE,NETW...
建立權杖物件	
修改物件標籤	
修改韌體環境值	Administrators
偵錯程式	Administrators
執行磁碟原維護工作	Administrators

使用者權限指派 (系統登入與關閉)



允許本機登入

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\允許本機登入

- 建議值

- Administrators, Users (群組)

- 說明

- 決定哪些使用者/群組可以登入電腦

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕本機登入

- 建議值

- Guests (群組)

- 說明

- 阻止哪些使用者/群組登入電腦

- 如果帳戶同時受限於[允許本機登入]與[拒絕本機登入]這兩種原則，此原則設定會取代 [允許本機登入] 原則設定

- 將此安全性原則套用到 Everyone 群組，將無人能夠登入本機



關閉系統

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\關閉系統

- 建議值

- Administrators, Users (群組)

- 說明

- 決定哪些本機登入電腦使用者/群組能將作業系統關機

使用者權限指派 (檔案存取權限)

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\取得檔案或其他物件的擁有權

- 建議值

- Administrators (群組)

- 說明

- 決定使用者能夠取得系統中任何檔案與物件之擁有權
 - 包括 Active Directory 物件、檔案及資料夾、印表機、登錄機碼、處理程序和執行緒
 - 物件擁有者將會擁有完全控制之權限

使用者權限指派 (網路存取權限)

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從網路存取這台電腦

- 建議值

- Administrators (群組)

- 說明

- 允許哪些使用者/群組可透過網路連線到這台電腦
 - 遠端桌面服務不受此原則影響

拒絕從網路存取這台電腦

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕從網路存取這台電腦

- 建議值

- Guests (群組)

- 說明

- 拒絕哪些使用者/群組從網路存取電腦

- 若使用者帳戶同時受限於 [從網路存取這台電腦] 與 [拒絕從網路存取這台電腦]，會以 [拒絕從網路存取這台電腦] 之原則設定為主



允許透過遠端桌面服務登入

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\允許透過遠端桌面服務登入

- 建議值

- Administrators, Remote Desktop Users (群組)

- 說明

- 決定哪些使用者/群組能以遠端桌面服務用戶端登入系統

使用者權限指派 (系統維護)



變更系統時間

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\變更系統時間

- 建議值

- Administrators, Local Service (群組)

- 說明

- 允許使用者/群組可變更系統時間

- 擁有此權限之使用者便可決定事件記錄檔之時間

- 若系統時間遭到變更，記錄的事件將會反映出新的時間，而非事件發生的實際時間



安全性選項

ICST

本機群組原則編輯器

檔案(F) 執行(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 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
- 使用者設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本

原則	安全性設定
DCOM: 以 Security Descriptor Definition Language (SDD...	尚未定義
DCOM: 以 Security Descriptor Definition Language (SDD...	尚未定義
Microsoft 網路用戶端: 傳送未加密的密碼到其他廠商的 SM...	已停用
Microsoft 網路用戶端: 數位簽章用戶端的通訊 (如果伺服器...	已啟用
Microsoft 網路用戶端: 數位簽章用戶端的通訊 (自動)	已停用
Microsoft 網路伺服器: 伺服器 SPN 目標名稱驗證層級	尚未定義
Microsoft 網路伺服器: 當登入時數到期時, 中斷用戶端連線	已啟用
Microsoft 網路伺服器: 數位簽章伺服器的通訊 (如果用戶端...	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: 不要求按 CTRL+ALT+DEL 鍵	尚未定義
互動式登入: 不要顯示上次登入的使用者名稱	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	14 天
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: 須有智慧卡	已停用
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
系統加密編譯: 使用 FIPS 相容演算法於加密, 雜湊, 以及簽章	已停用
系統加密編譯: 對使用者儲存在電腦上的金鑰強制使用增強...	尚未定義
系統物件: 加強內部系統物件的預設權限 (例如: 登錄簿)	已啟用

安全性選項 (帳戶)

帳戶：重新命名系統管理員帳戶

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名系統管理員帳戶

- 建議值

- Renamed_Admin

- 說明

- 重新命名已知的 Administrator 帳戶會使未經授權的人員較不容易猜出有此特殊權限的使用者名稱和密碼組合

- **機關依實務需求調整建議值**



帳戶：重新命名來賓帳戶名稱

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名來賓帳戶名稱

- 建議值

- Renamed_Guest

- 說明

- 重新命名已知的 Guest 帳戶會使未經授權的人員較不容易猜出此使用者名稱和密碼組合

- **機關依實務需求調整建議值**

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：Administrator 帳戶狀態

- 建議值

- 停用

- 說明

- 停用預設管理者帳戶

- 在停用 Administrator 帳戶後，欲重新啟用此帳戶，需重新輸入密碼。忘記密碼時，須由 Administrators 群組的替代成員，協助重設 Administrator 帳戶密碼



帳戶：Guest 帳戶狀態

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：Guest 帳戶狀態

- 建議值

- 停用

- 說明

- 停用來賓帳戶

安全性選項 (使用者帳戶控制)



標準使用者帳戶

ICST



使用者帳戶控制: 標準使用者之 提升權限提示的行為

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 標準使用者之提升權限提示的行為

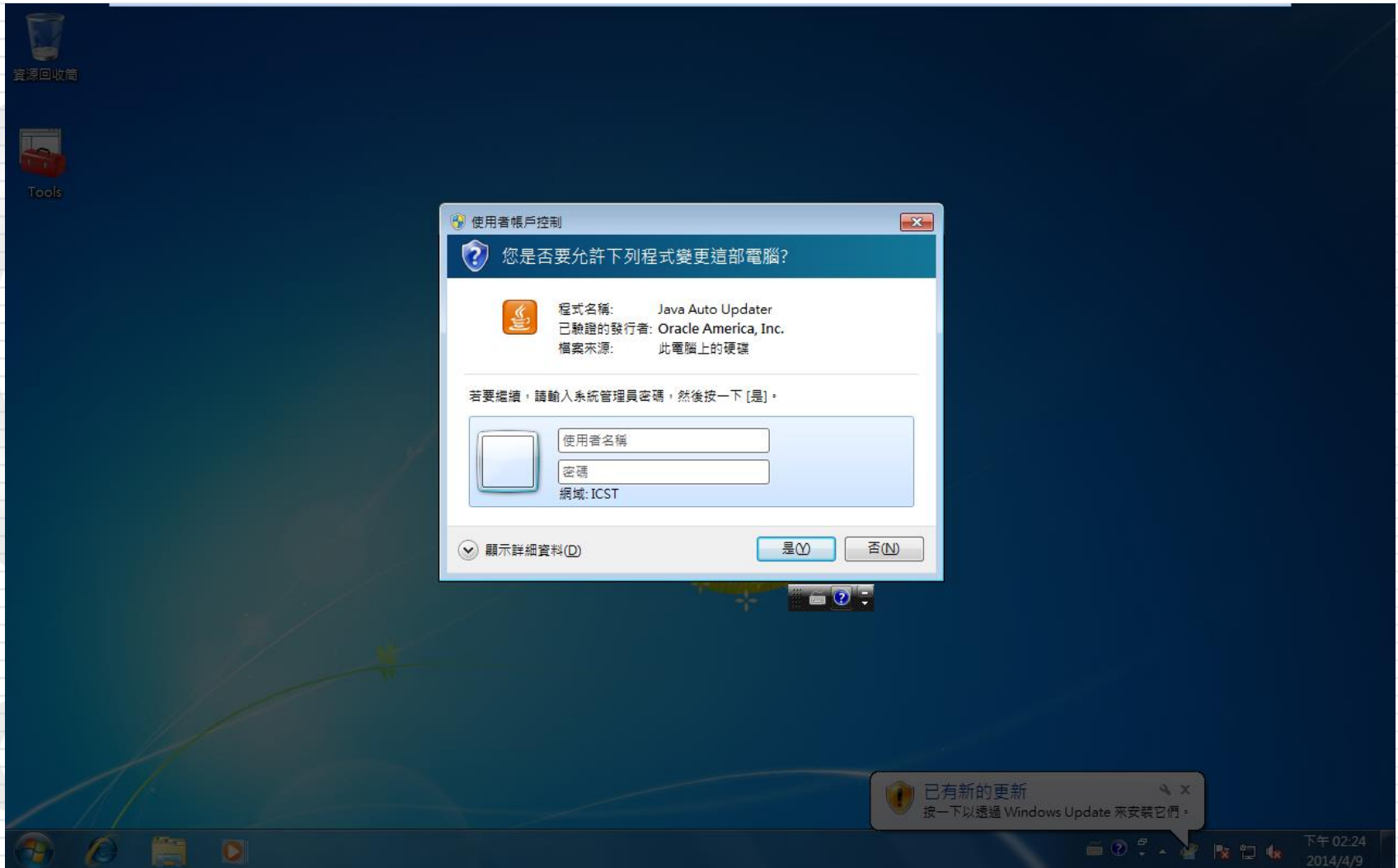
- 建議值

- 在安全桌面顯示輸入認證

- 說明

- 當操作需要提升權限時，會在安全桌面提示使用者輸入不同的使用者名稱與密碼

- 使用者輸入有效的認證，操作會以適用的權限繼續





系統管理員帳戶



使用者帳戶控制:使用內建的 Administrator 帳戶的管理員核准模式

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制:使用內建的 Administrator 帳戶的管理員核准模式

- 建議值

- 啟用

- 說明

- 若啟用原則，則使用內建的 Administrator 帳戶使用管理員核准模式

- 根據預設，任何需要提升權限的操作都會提示使用者核准操作



使用者帳戶控制: 所有系統管理員均以管理員核准模式執行

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 所有系統管理員均以管理員核准模式執行

- 建議值

- 啟用

- 說明

- 啟用原則，系統管理員任何需要提升權限的操作都會提示使用者核准操作



使用者帳戶控制:在管理員核准模式， 系統管理員之提升權限提示的行為

● 設定路徑

—電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制:在管理員核准模式，系統管理員之提升權限提示的行為

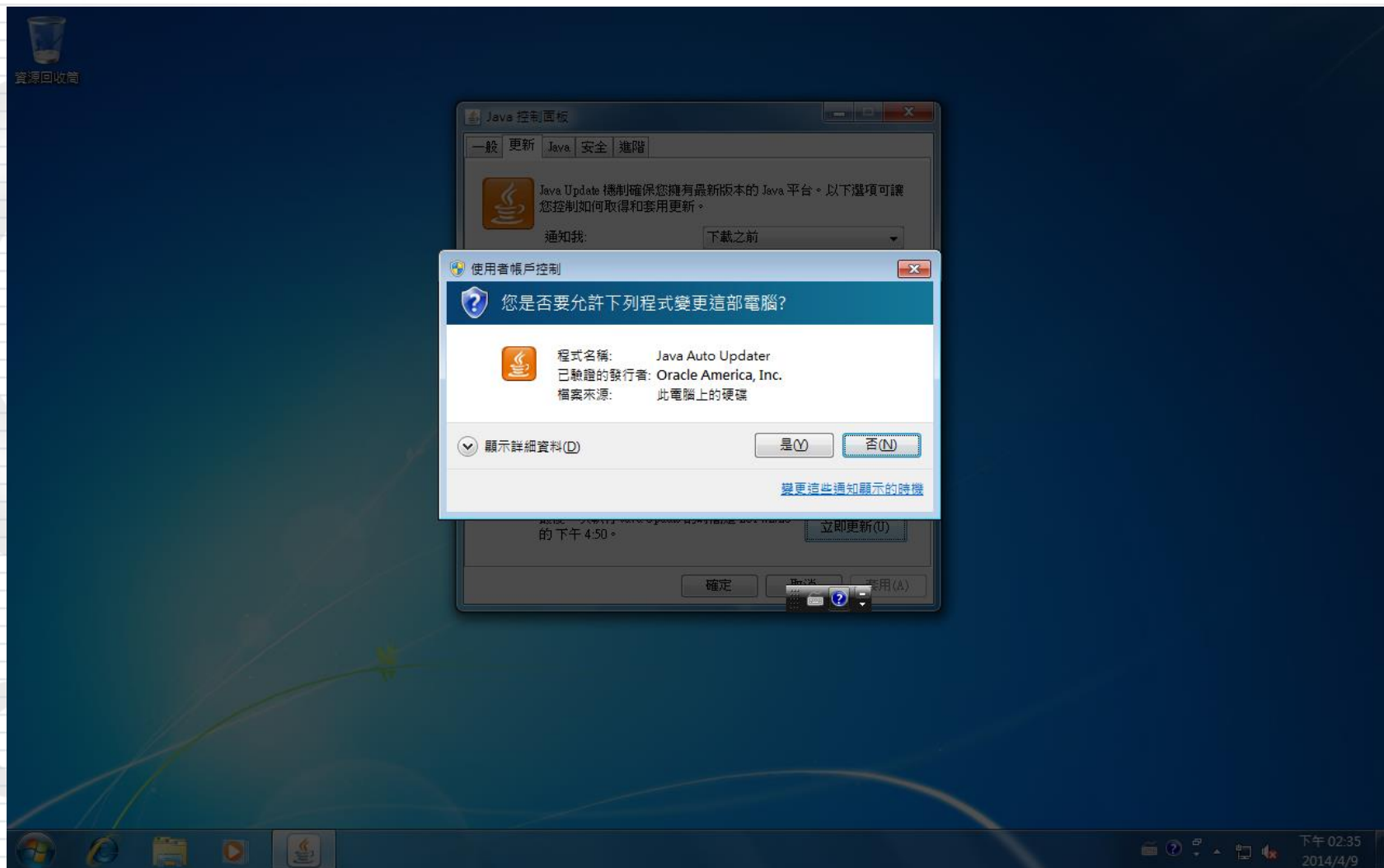
● 建議值

—提示要求同意

● 說明

—當操作需要提升權限時，會提示使用者選取 [允許] 或是 [拒絕]

—選取 [允許]，會以使用者的最高可用權限來進行操作





使用者帳戶控制: 偵測應用程式安裝，並提示提升權限

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 偵測應用程式安裝，並提示提升權限

- 建議值

- 啟用

- 說明

- 當偵測到應用程式安裝封裝需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼
- 輸入有效的認證，操作會以適用的權限繼續

安全性選項 (互動式登入)



互動式登入：在密碼到期前提示 使用者變更密碼

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入：在密碼到期前提示使用者變更密碼

- 建議值

- 14天

- 說明

- 在使用者密碼即將到期時，要提前多久(天數)事先提示使用者



互動式登入: 不要求按 CTRL+ALT+DEL 鍵

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入: 不要求按 CTRL+ALT+DEL 鍵

- 建議值

- 停用

- 說明

- 停用原則，則任何使用者都需要按 CTRL+ALT+DEL 才能登入 Windows (除非是使用智慧卡來登入 Windows)



互動式登入：不要顯示上次登入的使用者名稱

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入：不要顯示上次登入的使用者名稱

- 建議值

- 啟用

- 說明

- 啟用此原則，登入畫面不會顯示上次順利登入的使用者名稱

- 代表每次登入作業系統時，使用者必須輸入 [使用者帳戶名稱] 與 [使用者密碼]

安全性選項 (網路存取)

網路存取: 允許匿名 SID/名稱轉譯

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取: 允許匿名 SID/名稱轉譯

- 建議值

- 停用

- 說明

- 防止匿名使用者在取得系統管理員之SID後，能使用該SID來取得系統管理員的名稱



網路存取: 不允許存放網路驗證的密碼與認證

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取: 不允許存放網路驗證的密碼與認證

- 建議值

- 啟用

- 說明

- 不會在電腦上儲存網路驗證之密碼與認證資訊



網路存取: 不允許SAM帳戶和共用的匿名列舉

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取: 不允許SAM帳戶和共用的匿名列舉

- 建議值

- 啟用

- 說明

- 禁止匿名使用者執行[列舉網域帳戶]和[網路共用名稱]，可以避免遭人從網路上直接列舉出本機帳戶資料的風險



網路存取: 不允許 SAM 帳戶的匿名列舉

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取: 不允許 SAM 帳戶的匿名列舉

- 建議值

- 啟用

- 說明

- 禁止匿名使用者執行 [列舉網域帳戶]，可以避免遭人從網路上直接列舉出本機帳戶資料的風險

安全性選項 (網路安全性)



網路安全性: LAN Manager 驗證等級

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性: LAN Manager 驗證等級

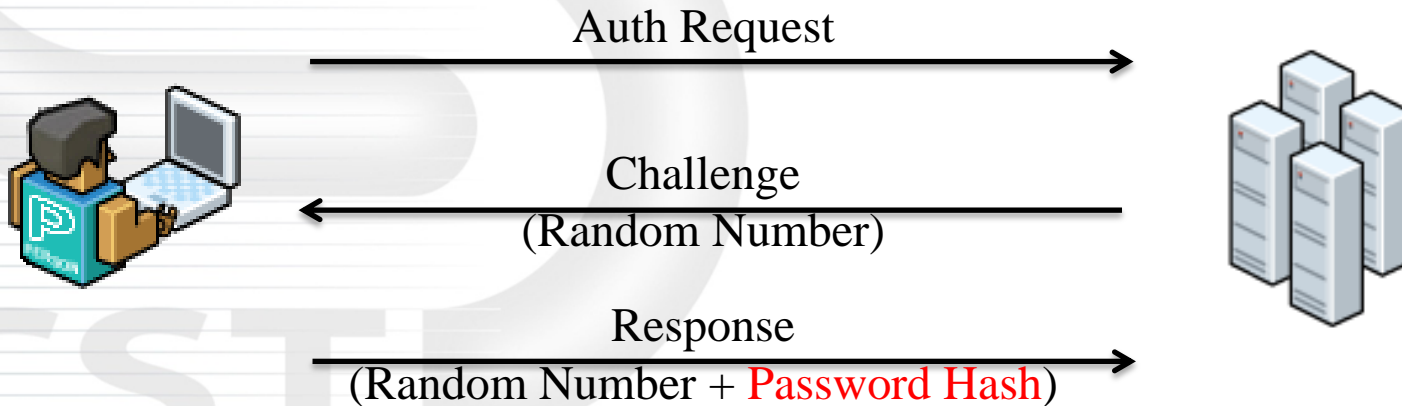
- 建議值

- 只傳送NTLMv2回應。拒絕LM和NTLM

- 說明

- 用戶端只使用 NTLMv2 驗證，而且若伺服器支援，則會使用 NTLMv2 工作階段安全性

- 利用身份認證協定取得遠端電腦的存取權限
 - LM, NTLMv1 (不安全)
 - NTLMv2, Kerberos (較安全)
- 使用 Challenge/Response 機制預防重送攻擊(Replay Attack)





網路安全性: 設定 Kerberos 允許的加密類型

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性: 設定 Kerberos 允許的加密類型

- 建議值

- RC4_HMAC_MD5
 - AES128_HMAC_SHA1
 - AES256_HMAC_SHA1
 - 未來的加密類型

- 說明

- 必須至少是 Windows 7 或 Windows Server 2008 R2 才支援此原則



網路安全性: 下次密碼變更時不 儲存 LAN Manager 雜湊數值

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性: 下次密碼變更時不儲存 LAN Manager 雜湊數值

- 建議值

- 啟用

- 說明

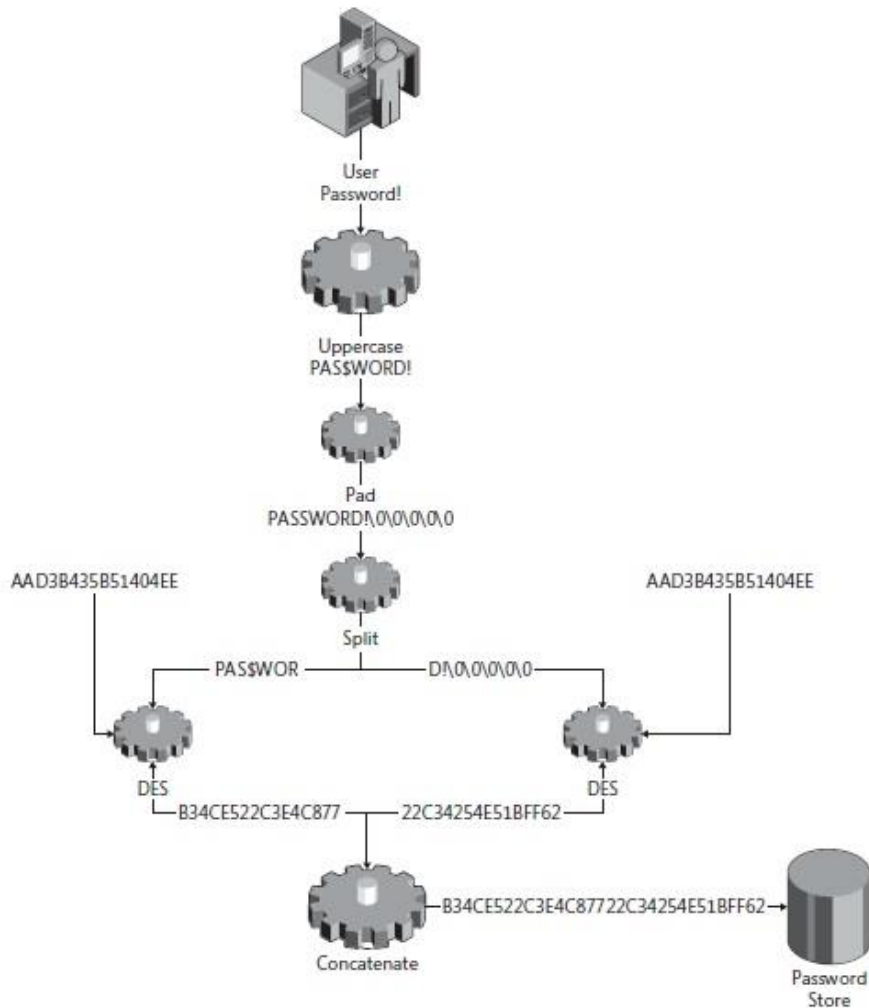
- 和加密編譯較強的 Windows NT 雜湊相比，LM 雜湊相對較不安全，並且容易遭到攻擊

- LM 雜湊儲存於本機電腦的安全性資料庫中，若安全性資料庫遭到攻擊，密碼可能就會被破解



LAN Manager 雜湊

LM 雜湊演算法



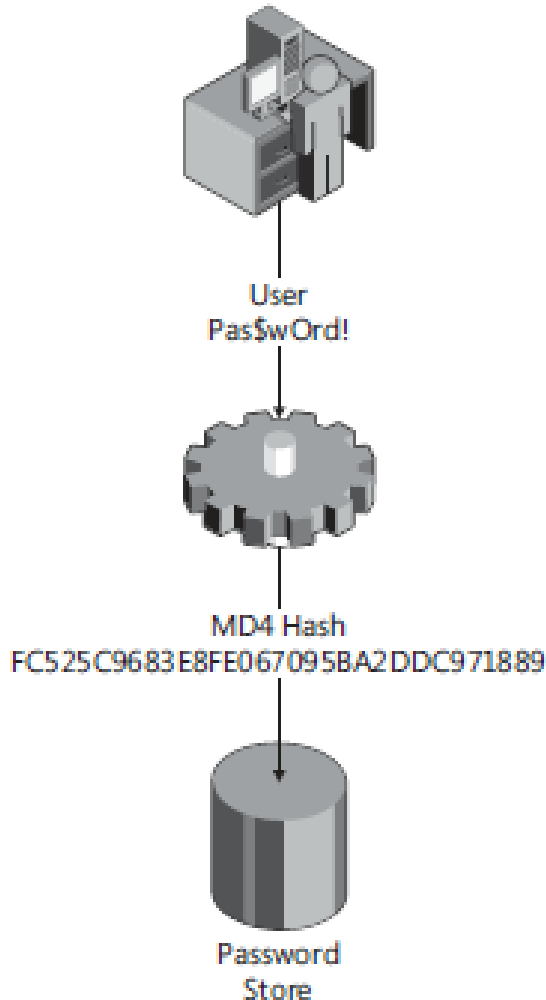
● 分段加密處理

- 全部轉為大寫
- 明文不足14個字元時，將使用 NULL補齊14個字元
- 將14個字元之密碼，均分為兩組(各7個字元)
- 將這兩組字元進行雜湊後之結果合併

● 密碼超過14字元

- LM雜湊法便無法使用

NTLM 雜湊演算法



- 將密碼透過 MD4 加密演算法進行加密
 - 保留所有密碼字元
 - 密碼字元長度最高可至 256 個字元



Windows 密碼儲存格式

- LAN Manager(LM) Hash
- Windows NT LAN Manager(NTLM) Hash

Format :

Username : SID : LM hash : NTLM hash : : :

LM hash



user:500:**E165F0192EF85EBBAAD3B435B51404EE** : **EB4FF39B74B0CBCE20A4F62DBD1E3585** :::



NTLM hash

```
Renamed_Admin:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Renamed_Guest:501:NO PASSWORD*****:NO PASSWORD*****
***:::
icst:1000:3E0E64AE92DE72309D6CC82FEE13AE59:F2A42A1817C161C6E20F5C1C1F3F2902:::
```

安全性選項 (Microsoft 網路伺服器)



Microsoft 網路伺服器: 暫停工作階段前, 要求的閒置時間

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器: 暫停工作階段前, 要求的閒置時間

- 建議值

- 15分鐘

- 說明

- 決定伺服器訊息區 (SMB) 工作階段的連續閒置時間長度超過多少時, 工作階段會因為處於非使用狀態而暫停
 - 若用戶端活動繼續, 則會自動重新建立工作階段



Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線

- 建議值

- 啟用

- 說明

- 在用戶端的登入時數到期之後，強迫將搭配 SMB 服務的用戶端工作階段中斷連線



Microsoft 網路用戶端: 傳送未加密的密碼到其他廠商的 SMB 伺服器

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路用戶端: 傳送未加密的密碼到其他廠商的 SMB 伺服器

- 建議值

- 停用

- 說明

- 停用原則，便禁止將純文字密碼傳送給不支援密碼加密的非 Microsoft SMB (第三方) 伺服器

安全性選項 (系統加密編譯)



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

● 設定路徑

- 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\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

● 建議值

- 啟用

● 說明

- 啟用此設定，傳輸層安全性/安全通訊端層(TLS/SSL)安全性提供者只會使用FIPS 140核准的加密編譯演算法
- 3DES與AES用於加密，安全雜湊演算法用於TLS雜湊
- RSA或ECC公開金鑰加密編譯用於TLS金鑰交換與驗證

網際網路通訊設定

本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - Windows 元件
 - 印表機
 - 系統
 - 網路 (highlighted in red box)
 - BranchCache
 - DNS 用戶端
 - LanMan 伺服器
 - Microsoft 對等網路服務
 - QoS 封包排程器
 - SNMP
 - SSL 組態設定
 - TCPIP 設定值
 - Windows Connect Now
 - 背景智慧型傳送服務 (BITS)
 - 連結階層拓樸搜索
 - 網路連線
 - 網路連線狀態指示器
 - 離線檔案

- 所有設定
- 使用者設定
- 軟體設定
- Windows 設定
- 系統管理範本

網路

選取一個項目來檢視它的描述。

設定	狀態
BranchCache	
DNS 用戶端	
LanMan 伺服器	
Microsoft 對等網路服務	
QoS 封包排程器	
SNMP	
SSL 組態設定	
TCPIP 設定值	
Windows Connect Now	
背景智慧型傳送服務 (BITS)	
連結階層拓樸搜索	
網路連線	
網路連線狀態指示器	
離線檔案	
設定 DFS 用戶端搜尋 DC 的頻率	尚未設定



要求網域使用者在設定網路的位置時必須提升權限(1/2)

- 設定路徑

- 電腦設定\系統管理範本\網路\網路連線\要求網域使用者在設定網路的位置時必須提升權限

- 建議值

- 啟用

- 說明

- 啟用原則，網域使用者在設定網路位置時必須提升權限
 - 網路位置包含：工作場所區域、公用網路及家用網路

要求網域使用者在設定網路的位置時必須提升權限(2/2)

● 設定圖示

此電腦已連線到網路。Windows 將會根據網路的位置自動套用正確的網路設定。



家用網路

如果此網路上的所有電腦都在您家中，而且您認得它們，則這是受信任的家用網路。請勿在公共場所 (例如，咖啡廳或機場) 選擇這個選項。



工作場所網路

如果此網路上的所有電腦均位於您的工作場所中，而且您認得它們，則這是受信任的工作場所網路。請勿在公共場所 (例如，咖啡廳或機場) 選擇這個選項。



公用網路

如果您不認得網路上的所有電腦 (例如，在咖啡廳或機場，或是您使用行動式寬頻)，則這是公用網路並且不受信任。

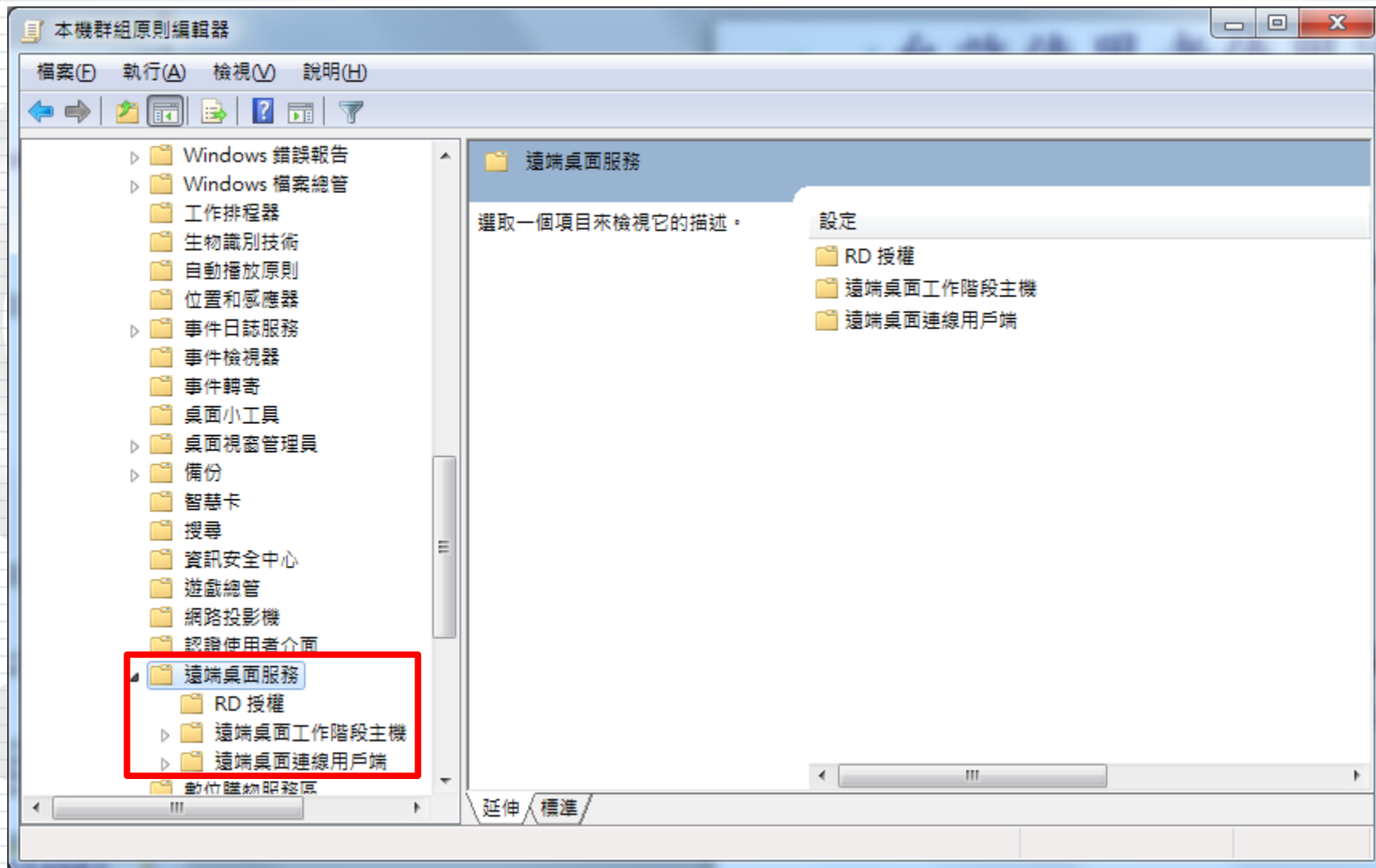
將我未來連線的所有網路視為公用，以後不要再詢問我。

[協助我選擇](#)



遠端桌面服務

ICST





允許使用者使用遠端桌面服務從 遠端連線

- 設定路徑

- 電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\連線\允許使用者使用遠端桌面服務從遠端連線

- 建議值

- 停用

- 說明

- 停用原則，使用者即無法使用遠端桌面服務，從遠端連線至目標電腦
 - 已建立之連線會持續保持連線，但不再接受任何新連線

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\遠端桌面服務\遠端桌面工作階段主機\安全性\連線時永遠提示密碼

- 建議值

- 啟用

- 說明

- 根據預設，遠端桌面服務允許使用者在遠端桌面連線用戶端程式中輸入密碼，即可自動登入

- 啟用設定後，即使已在遠端桌面連線用戶端中提供密碼，也不能自動登入遠端桌面服務。即登入前會再次要求輸入密碼

不允許儲存密碼

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\遠端桌面服務\遠端桌面連線用戶端\不允許儲存密碼

- 建議值

- 啟用

- 說明

- 啟用設定，[遠端桌面連線(用戶端程式)] 之密碼儲存核取方塊將會停用，再也無法儲存密碼

- 所有先前存在於 RDP 檔案中的密碼都將予以刪除



設定用戶端連線加密層級

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\遠端桌面服務\遠端桌面工作階段主機\安全性\設定用戶端連線加密層級

- 建議值

- 啟用

- 高等級

- 說明

- 在遠端連線期間，用戶端與 RDP工作階段主機伺服器之間的所有通訊都會使用增強式128位元加密



為使用中但閒置的遠端桌面服務 工作階段設定時間限制

● 設定路徑

– 電腦設定\系統管理範本\Windows元件\遠端桌面服務\遠端桌面工作階段主機\工作階段時間限制\為使用中但閒置的遠端桌面服務工作階段設定時間限制

● 建議值

– 啟用

➤ 15分鐘

● 說明

– 於設定之閒置時間前 (2分鐘)，遠端連線之使用者會收到斷線通知

– 閒置之連線將於設定時間到達後，隨即斷線

設定已斷線工作階段的時間限制

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\遠端桌面服務\遠端桌面工作階段主機\工作階段時間限制\設定已斷線工作階段的時間限制

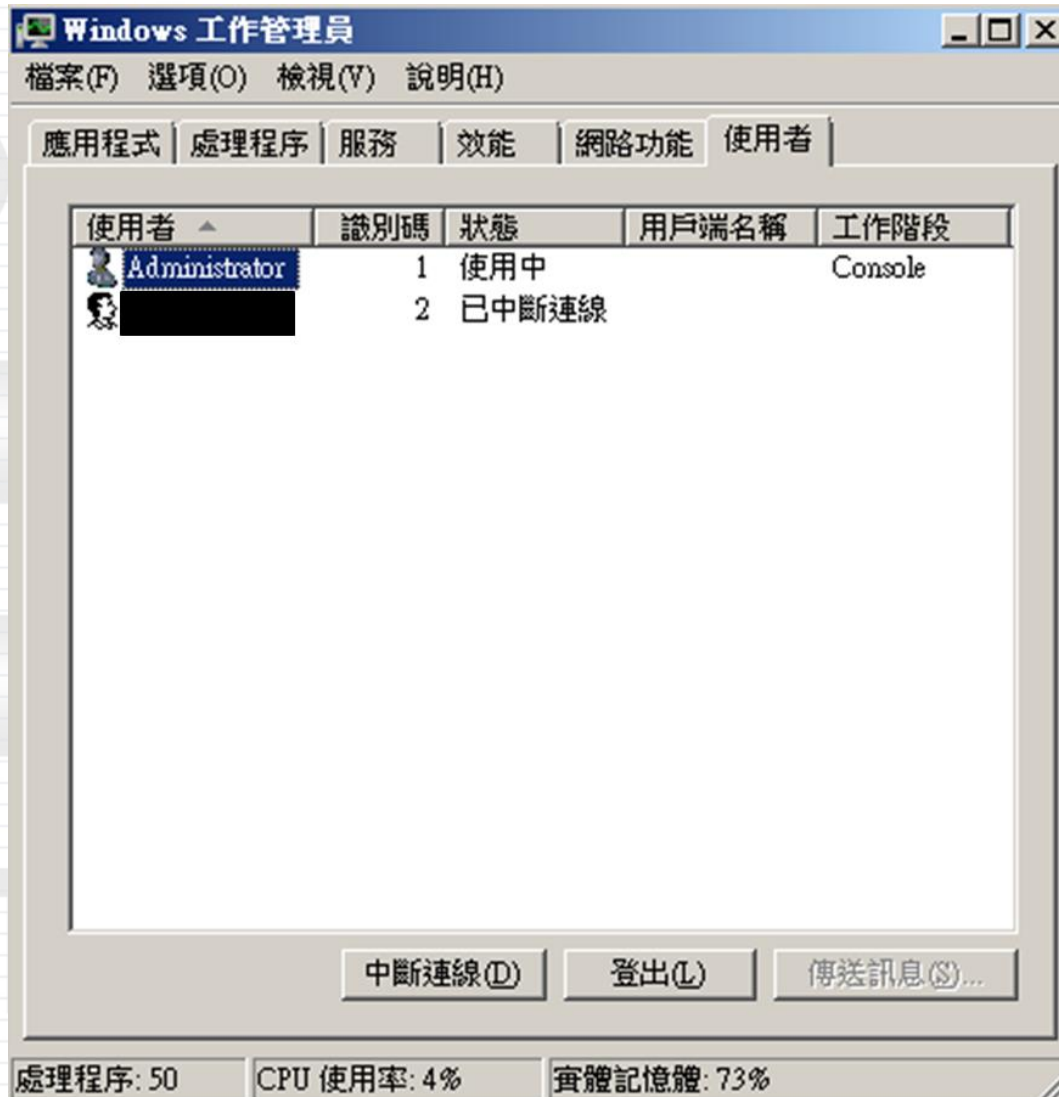
- 建議值

- 啟用

- 1分鐘

- 說明

- 已中斷之連線，在經過指定時間後便會刪除此工作階段



Windows 工作管理員

檔案(F) 選項(O) 檢視(V) 說明(H)

應用程式 | 處理程序 | 服務 | 效能 | 網路功能 | 使用者

使用者	識別碼	狀態	用戶端名稱	工作階段
Administrator	1	使用中		Console
[Redacted]	2	已中斷連線		

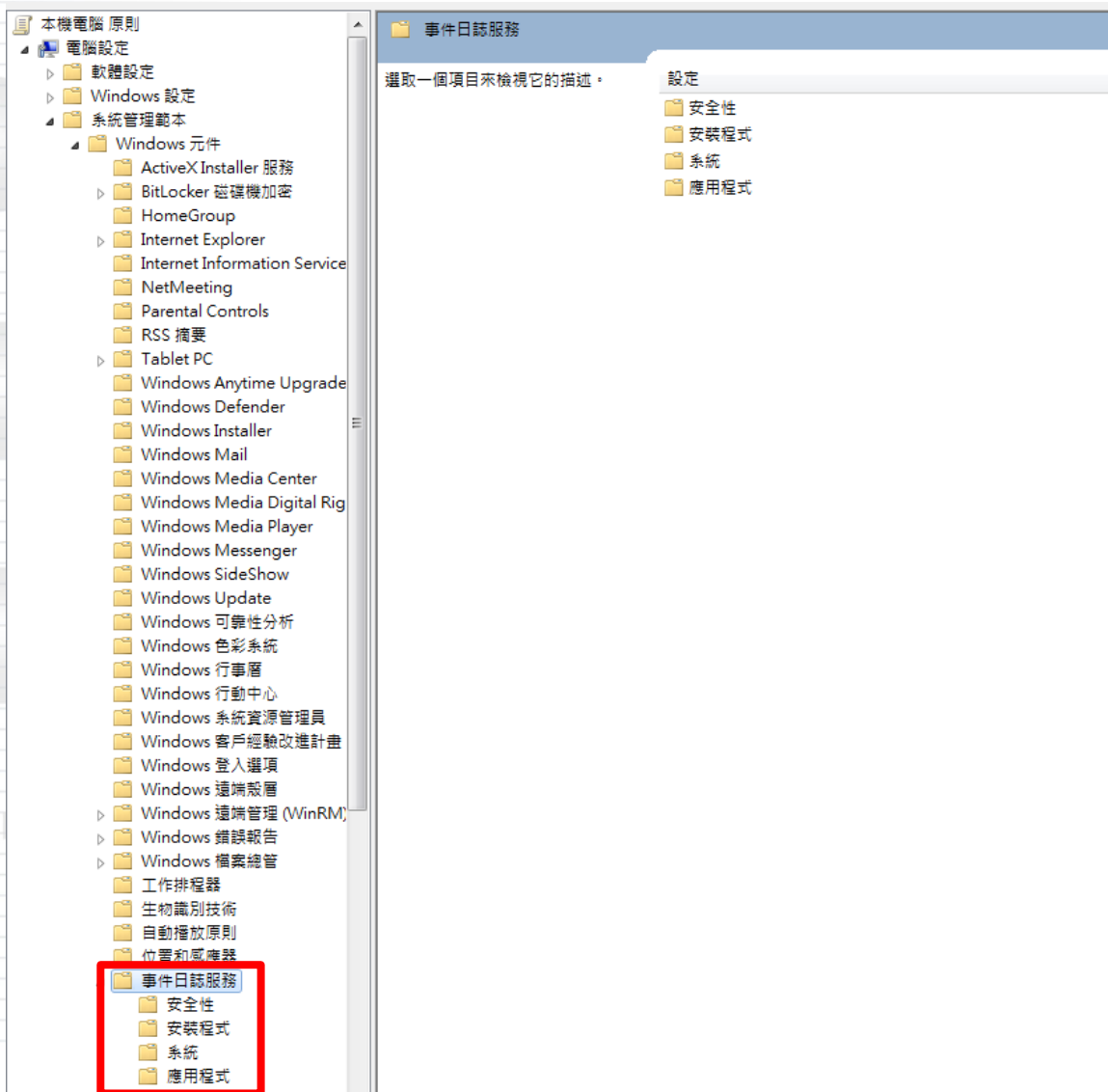
中斷連線(D) | 登出(L) | 傳送訊息(S)...

處理程序: 50 | CPU 使用率: 4% | 實體記憶體: 73%



事件日誌服務

ICST





記錄檔大小上限(KB) (1/2)

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\事件日誌服務\應用程式\記錄檔大小上限(KB)

- 建議值

- 啟用

- 記錄檔大小上限：32,768~81,920(KB) (即32~80MB)

- 說明

- 指定記錄檔的大小上限 (以 KB 為單位)

- 數值範圍：1 MB (1024 KB) ~ 2 TB (2147483647 KB)



記錄檔大小上限(KB) (2/2)

- 記錄檔大小上限設定

事件日誌服務 /安全性	事件日誌服務 /安裝程式	事件日誌服務 /系統	事件日誌服務 /應用程式
81,920 (KB)	32,768 (KB)	32,768 (KB)	32,768 (KB)



系統

ICST

本機群組原則編輯器

檔案(F) 執行(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
 - 軟體設定
 - Windows 設定
 - 系統管理範本
 - Windows 元件
 - 系統 (highlighted)
 - iSCSI
 - Kerberos
 - Windows HotStart
 - Windows 時間服務
 - Windows 檔案保護
 - 分散式 COM
 - 可信賴平台模組服務
 - 地區設定服務
 - 系統還原
 - 使用者設定檔
 - 卸除式儲存裝置存取權
 - 指令碼
 - 效能控制台
 - 復原
 - 登入
 - 群組原則
 - 裝置安裝
 - 裝置重新導向
 - 資料夾重新導向
 - 電源管理
 - 疑難排解與診斷
 - 磁碟 NV 快取
 - 磁碟配額
 - 網路登入
 - 網路網路通訊管理
 - 認證委派
 - 遠端協助
 - 遠端程序呼叫
 - 增強的存放區存取
 - 檔案系統
 - 關機選項
 - 驅動程式安裝
 - 網路
 - 所有設定

使用者設定

- 軟體設定
- Windows 設定
- 系統管理範本

系統

選取一個項目來檢視它的描述。

設定	狀態	註解
iSCSI		
Kerberos		
Windows HotStart		
Windows 時間服務		
Windows 檔案保護		
分散式 COM		
可信賴平台模組服務		
地區設定服務		
系統還原		
使用者設定檔		
卸除式儲存裝置存取權		
指令碼		
效能控制台		
復原		
登入		
群組原則		
裝置安裝		
裝置重新導向		
資料夾重新導向		
電源管理		
疑難排解與診斷		
磁碟 NV 快取		
磁碟配額		
網路登入		
網路網路通訊管理		
認證委派		
遠端協助		
遠端程序呼叫		
增強的存放區存取		
檔案系統		
關機選項		
驅動程式安裝		
下載遺失的 COM 元件	尚未設定	否
允許啟用作式連結追蹤用戶端使用網域資源	尚未設定	否
不要將移到已加密資料夾中的檔案自動加密	尚未設定	否
在發生 Windows 系統關機後不要關閉系統電源	尚未設定	否
啟用持續的時間戳記	尚未設定	否
啟動關機事件追蹤器系統狀態資料功能	尚未設定	否
顯示關機事件追蹤器	尚未設定	否
關閉 HTML Help 可執行檔的資料執行防止	尚未設定	否
將可能不安全的 HTML 說明功能限制於指定的資料夾	尚未設定	否

14 個設定

允許遠端存取隨插即用介面

- 設定路徑

- 電腦設定\系統管理範本\系統\裝置安裝\允許遠端存取隨插即用介面

- 建議值

- 停用

- 說明

- 不允許從遠端連線到隨插即用介面

- 設定路徑

- 電腦設定\系統管理範本\系統\裝置安裝\在通常會提示 Windows 建立系統還原點的裝置活動期間，防止 Windows 建立系統還原點

- 建議值

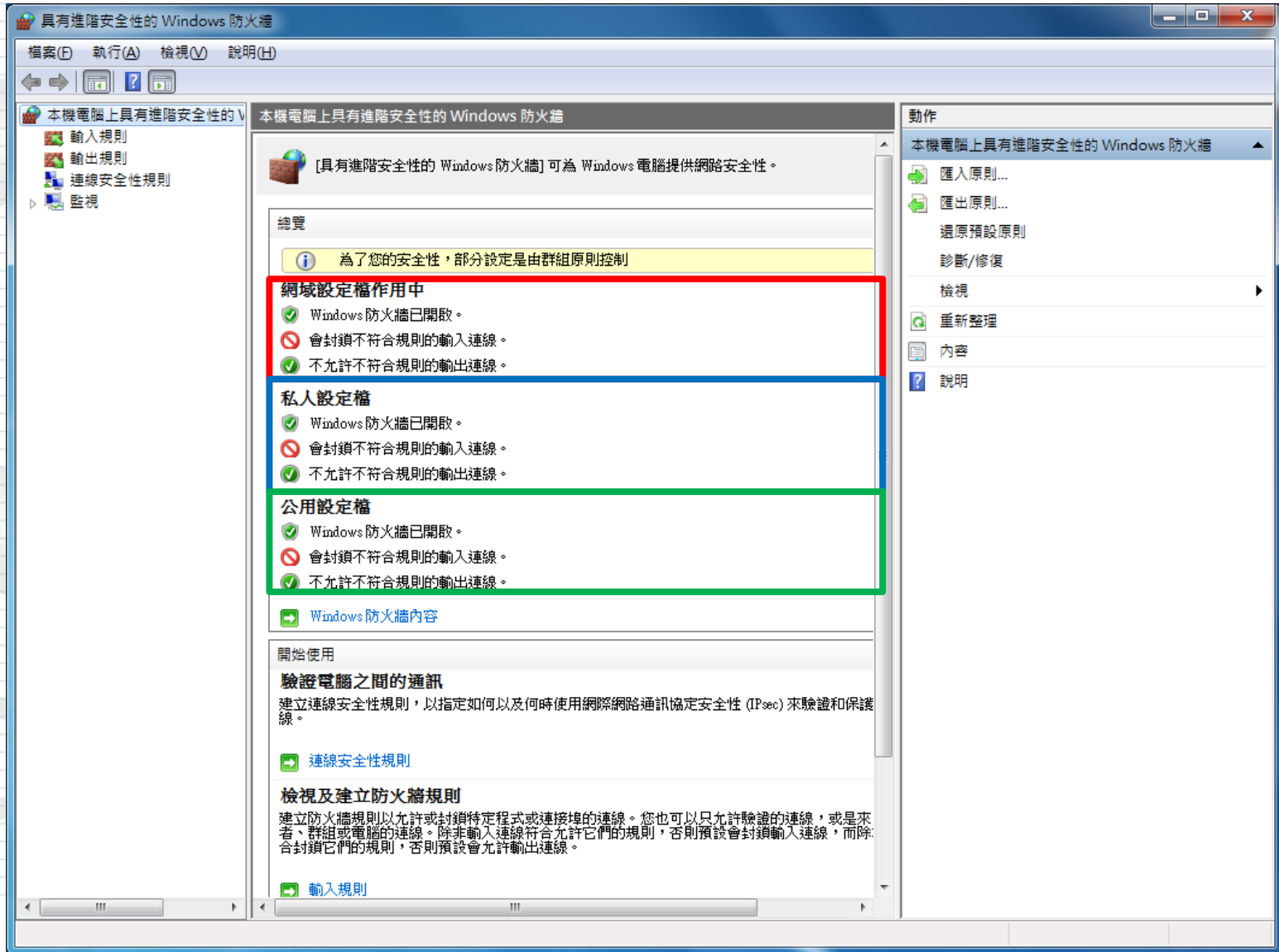
- 停用

- 說明

- 停用原則，系統便會為部分驅動程式活動 (如：安裝未經簽署的驅動程式) 建立系統還原點



Windows 防火牆



具有進階安全性的 Windows 防火牆

本機電腦上具有進階安全性的 Windows 防火牆

[具有進階安全性的 Windows 防火牆] 可為 Windows 電腦提供網路安全性。

總覽

為了您的安全性，部分設定是由群組原則控制

網域設定檔作用中

- Windows 防火牆已開啟。
- 會封鎖不符合規則的輸入連線。
- 不允許不符合規則的輸出連線。

私人設定檔

- Windows 防火牆已開啟。
- 會封鎖不符合規則的輸入連線。
- 不允許不符合規則的輸出連線。

公用設定檔

- Windows 防火牆已開啟。
- 會封鎖不符合規則的輸入連線。
- 不允許不符合規則的輸出連線。

Windows 防火牆內容

開始使用

驗證電腦之間的通訊

建立連線安全性規則，以指定如何以及何時使用網際網路通訊協定安全性 (IPsec) 來驗證和保護連線。

連線安全性規則

檢視及建立防火牆規則

建立防火牆規則以允許或封鎖特定程式或連接埠的連線。您也可以只允許驗證的連線，或是來者、群組或電腦的連線。除非輸入連線符合允許它們的規則，否則預設會封鎖輸入連線，而除封鎖它們的規則，否則預設會允許輸出連線。

輸入規則

動作

- 本機電腦上具有進階安全性的 Windows 防火牆
- 匯入原則...
- 匯出原則...
- 還原預設原則
- 診斷/修復
- 檢視
- 重新整理
- 內容
- 說明

Windows 防火牆

(防火牆設定)



Windows 防火牆: 保護所有網路 連線

- 設定路徑

- 電腦設定\系統管理範本\網路\網路連線\Windows 防火牆\
網域設定檔\Windows 防火牆: 保護所有網路連線

- 建議值

- 啟用

- 說明

- 開啟 Windows 防火牆

Windows防火牆 (連線管控設定)

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的
Windows 防火牆\內容\網域設定檔\輸出連線

- 建議值

- 允許(預設)

- 說明

- 控制Windows 防火牆對於輸出連線的預設行為
 - 允許防火牆內部對防火牆外部之網路連線

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的
Windows 防火牆\內容\網域設定檔\輸入連線

- 建議值

- 封鎖(預設)

- 說明

- 控制Windows 防火牆對於輸入連線的預設行為
 - 阻擋防火牆外部對防火牆內部之網路連線

套用本機防火牆規則

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\網域設定檔\自訂\規則合併\套用本機防火牆規則

- 建議值

- 否

- 說明

- 禁止套用本機系統管理員所建立的本機防火牆規則

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\網域設定檔\自訂\規則合併\套用本機連線安全性規則

- 建議值

- 否

- 說明

- 不允許套用本機系統管理員所建立的本機連線安全性規則



Windows防火牆:禁止單點傳送 回應到多點傳送或廣播要求

- 設定路徑

- 電腦設定\系統管理範本\網路\網路連線\Windows防火牆\網域設定檔\Windows防火牆:禁止單點傳送回應到多點傳送或廣播要求

- 建議值

- 啟用

- 說明

- 禁止系統針對多點傳送或廣播之要求(Request) 進行回應(Response)

Windows防火牆 (輸入規則)



核心網路功能-動態主機設定通訊協定 (DHCP-In)

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\輸入規則\核心網路功能-動態主機設定通訊協定 (DHCP-In)

- 建議值

- 啟用

- 說明

- 允許全狀態自動配置(Stateful auto-configuration)的DHCP(動態主機設定通訊協定)訊息



核心網路功能-IPv6 的動態主機設定 通訊協定 (DHCPV6-In)

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\輸入規則\核心網路功能-IPv6 的動態主機設定通訊協定 (DHCPV6-In)

- 建議值

- 啟用

- 說明

- 允許全狀態自動配置(Stateful auto-configuration)與無狀態自動配置(Stateless auto-configuration)的 DHCPV6 (IPv6的動態主機設定通訊協定)訊息

Windows防火牆 (防火牆通知設定)

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\網域設定檔\自訂\防火牆設定\顯示通知

- 建議值

- 是

- 說明

- 當程式接收輸入連線而遭防火牆封鎖時，防火牆即顯示通知告知使用者

- 設定路徑

- 電腦設定\系統管理範本\網路\網路連線\Windows 防火牆\網域設定檔\Windows 防火牆: 禁止通知

- 建議值

- 停用

- 說明

- 程式要求 Windows 防火牆將程式新增到程式例外清單上時，Windows 防火牆就會允許顯示這些通知

允許通過防火牆之程式

允許程式通過 Windows 防火牆通訊

若要新增、變更或移除允許的程式與連接埠，請按一下 [變更設定]。

允許程式通訊的風險為何？

變更設定(N)

為了您的安全，部分設定已由您的系統管理員管理。

允許的程式與功能(A):

名稱	網域	家用/工作場所 (...)	公用	群組原則
<input type="checkbox"/> BranchCache - 內容抓取 (使用 HTTP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> BranchCache - 同儕節點探索 (使用 WSD)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> BranchCache - 託管快取用戶端 (使用 HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> BranchCache - 託管快取伺服器 (使用 HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input checked="" type="checkbox"/> Environment Sensor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> Environment Sensor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> HomeGroup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> iSCSI 服務	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input type="checkbox"/> Media Center Extender	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否
<input checked="" type="checkbox"/> Microsoft Office Outlook	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	否
<input checked="" type="checkbox"/> Microsoft Office Outlook	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	否

詳細資料(L)...

移除(M)

允許其他程式(R)...

防火牆狀態與通知

自訂每個網路類型的設定

您可以為您使用的每個網路位置類型修改防火牆設定。

什麼是網路位置？

為了您的安全，部分設定已由您的系統管理員管理。

網域網路位置設定

- 開啟 Windows 防火牆
 - 封鎖所有連入連線，包括允許的程式清單中的連入連線
 - 當 Windows 防火牆封鎖新的程式時請通知我
- 關閉 Windows 防火牆 (不建議)

家用或工作場所 (私人) 網路位置設定

- 開啟 Windows 防火牆
 - 封鎖所有連入連線，包括允許的程式清單中的連入連線
 - 當 Windows 防火牆封鎖新的程式時請通知我
- 關閉 Windows 防火牆 (不建議)

公用網路位置設定

- 開啟 Windows 防火牆
 - 封鎖所有連入連線，包括允許的程式清單中的連入連線
 - 當 Windows 防火牆封鎖新的程式時請通知我
- 關閉 Windows 防火牆 (不建議)

Windows防火牆 (記錄檔設定)

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的
Windows 防火牆\內容\網域設定檔\記錄\名稱

- 建議值

- %windir%\system32\logfiles\firewall\domainfirewall.log

- 說明

- 設定 Windows 防火牆記錄檔的名稱

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的
Windows 防火牆\內容\網域設定檔\記錄\大小限制

- 建議值

- 16384 (KB)

- 說明

- 設定 Windows 防火牆 記錄檔的大小

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\網域設定檔\記錄\記錄成功的連線

- 建議值

- 是

- 說明

- 啟用原則，Windows 防火牆將記錄成功之連線

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\網域設定檔\記錄\記錄丟棄的封包

- 建議值

- 是

- 說明

- 啟用原則，Windows 防火牆將記錄丟棄的封包

報告完畢
敬請指教