|  |  |  |
| --- | --- | --- |
|  | | |
| **政府組態基準**  **Microsoft Windows 10**  **TWGCB-01-005**  **(V1.4)** | | |
|  |  |  |
|  | | |
| 行政院國家資通安全會報技術服務中心  中華民國110年10月 | | |

**修訂歷史紀錄表**

| 項次 | 版次 | 修訂日期 | 說明 |
| --- | --- | --- | --- |
| 1 | 1.0 | 107/1/29 | 新編 |
| 2 | 1.1 | 108/12/17 | * 修改表2項次1、24、38、42、54、55、81、83、101、102、103、104、105、108、111、119、160、162、165、175、218、222、228、233、235、236、240、268、270、274、282、284、285、287及291之說明內容 * 表2項次38之CCE-ID由「CCE-35095-9」修改為「CCE-44437-2」 * 表2項次38之原則設定名稱，由「開啟PIN登入」修改為「開啟方便的PIN登入」 * 表2項次48之原則設定名稱，由「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」修改為「在通常會提示建立系統還原點的裝置活動期間，防止建立系統還原點」 * 表2項次55之原則設定名稱，由「關閉市集的存取權」修改為「關閉Microsoft Store的存取權」 * 表2項次69之原則設定名稱，由「關閉Windows Messenger客戶經驗改善計畫」修改為「關閉Windows Messenger客戶經驗改進計畫」 * 表2項次75與76之GPO設定路徑，由「電腦設定\Windows設定\安全性設定\進階稽核原則設定\稽核原則\...」修改為「電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\...」 * 表2項次84之原則設定名稱，由「稽核原則：系統：稽核IPSEC驅動程式」修改為「稽核原則：系統：稽核IPsec驅動程式」 * 表2項次85之原則設定名稱，由「稽核原則:系統:稽核其他系統事件」修改為「稽核原則：系統：稽核其他系統事件」 * 表2項次99之原則設定名稱，由「裝置：允許格式化以及退出卸除式媒體」修改為「裝置：允許格式化以及退出抽取式媒體」 * 表2項次109之原則設定名稱，由「互動式登入：不要顯示上次登入的使用者名稱」修改為「互動式登入：不要顯示上次登入」 * 表2項次111之原則設定名稱，由「互動式登入：電腦帳戶閾值」修改為「互動式登入：電腦帳戶鎖定閾值」 * 表2項次165之原則設定名稱，由「系統加密編譯 ：使用FIPS相容演算法於加密、雜湊以及簽章」修改為「系統密碼編譯 ：使用FIPS相容演算法於加密、雜湊以及簽章」 * 表2項次168之「使用者帳戶控制：使用內建的Administrator帳戶的管理員核准模式」設定值，由「在安全桌面提示要求同意」修改為「啟用」 * 表2項次169之原則設定名稱，由「系使用者帳戶控制：允許UIAccess應用程式不使用安全桌面來提升權限」修改為「使用者帳戶控制：允許UIAccess應用程式不使用安全桌面來提示提升權限」 * 表2項次172之原則設定名稱，由「使用者帳戶控制：偵測應用程式安裝，並提示提升權限」修改調整為「使用者帳戶控制：偵測應用程式安裝，並提示提高權限」 * 表2項次207之「以服務方式登入」設定值，由「Guests」修改為「No One」 * 表2項次225之原則設定名稱，由「限制解壓縮和安裝未經數位簽署的小工具」修改為「限制解壓縮和安裝未經過數位簽署的小工具」 * 表2項次237之原則設定名稱，由「防止出現Windows Installer指令碼的IE安全性提示」修改為「防止出現Windows Installer指令碼的Internet Explorer 安全性提示」 * 表2項次263之「重新排程已經排程好的自動更新安裝」設定值，由「啟用，分鐘」修改為「啟用，1分鐘」 * 表2項次265之原則設定名稱，由「允許基本驗證」修改為「允許基本驗證(用戶端)」 * 表2項次270之原則設定名稱，由「設定Windows Smart Screen篩選工具」修改為「設定Windows Smart Screen」 * 表2項次276之原則設定名稱，由「系統起始的重新啟動系統之後自動登入最後一個互動式使用者」修改為「在重新開機後，自動登入並鎖定最後一個互動式使用者 」 * 表2項次282之原則設定名稱，由「防止電腦加入Home Group」修改為「防止電腦加入家用群組」 * 表2項次284之原則設定名稱，由「關閉市集應用程式」修改為「關閉Microsoft Store應用程式」 * 表2項次285之原則設定名稱，由「停用Windows市集中的所有應用程式」修改為「停用來自Microsoft Store的所有應用程式」 * 表2項次286之原則設定名稱，由「允許基本驗證」修改為「允許基本驗證(服務)」 * 表2項次287之原則設定名稱，由「加入Microsoft MAPS」修改為「加入Microsoft MAPS」 * 表2項次298之原則設定名稱，由「封鎖未授信任的字型」修改為「封鎖未受信任的字型」 * 表2項次313之GPO設定路徑，由「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(網域)」修改為「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」 * 表2項次345之「名稱(公用)」設定值，由「%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log」修改為「%windir%\system32\logfiles\firewall\publicfirewall.log」 |
| 3 | 1.2 | 109/2/11 | * 新增表2項次232「關閉Windows Mail應用程式」之備註「適用1709以前版本」 * 新增表2項次233「關閉社群功能」之備註「適用1709以前版本」 * 新增表2項次274「關閉遊戲資訊下載」之備註「適用1803以前版本」 * 新增表2項次275「關閉遊戲更新」之備註「適用1803以前版本」 * 表2項次271與272之GPO設定路徑，由「電腦設定\系統管理範本\Windows元件\Windows檔案總管\」修改為「電腦設定\系統管理範本\Windows元件\檔案總管\」 |
| 4 | 1.3 | 109/11/24 | 修改表2項次2「密碼最長使用期限」之說明內容 |
| 5 | 1.4 | 110/10/5 | * 表2項次22、23及24之說明內容，由「原則預設狀態」修改為「預設狀態」 * 表2項次22、23及24之說明內容，由「原則啟用狀態」修改為「啟用狀態」 * 表2項次22、23及24之說明內容，由「原則停用狀態」修改為「停用狀態」 * 表2項次31之說明內容，由「不良，但為開機所需」修改為「不良但關鍵」 * 表2項次42、43、96、98、116、146、155、157、178、179、182、196及251內容說明刪除對Windows 10前之舊版作業系統提醒事項 * 表2項次105之說明內容，由「篡」修改為「竄」 * 表2項次116之說明內容，由「無動作」修改為「沒有動作」 * 表2項次150之說明內容，由「傳統」修改為「傳統，本機使用者以自身身分驗證」 * 表2項次150之說明內容，由「僅適用於來賓」修改為「僅適用於來賓，本機使用者以Guest驗證」 * 表2項次237之說明內容，由「企業」修改為「機關」 * 表2項次253之說明內容，由「高」修改為「高等級」 * 表2項次253之說明內容，由「低」修改為「低等級」 * 表2項次260之說明內容，由「指定內部網路Microsoft更新服務位置」修改為「指定近端內部網路Microsoft更新服務的位置」 * 新增36項與修改129項設定項目，異動內容詳見附件1 |
|  | | | |

**目　次**

[1. 前言 1](#_Toc85103631)

[1.1 適用環境 1](#_Toc85103632)

[1.2 項數統計 1](#_Toc85103633)

[1.3 文件發行 1](#_Toc85103634)

[2. Windows 10政府組態基準列表 2](#_Toc85103635)

[3. 參考文獻 299](#_Toc85103636)

[4. 附件 300](#_Toc85103637)

[附件1 版次1.4異動設定項目列表 附件1-1](#_Toc85103638)

**表 目 次**

[表1 Windows 10組態基準項目統計 1](#_Toc64420136)

[表2 Windows 10政府組態基準列表 2](#_Toc64420137)

# 前言

政府組態基準(Government Configuration Baseline, 以下簡稱GCB)目的在於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。

## 適用環境

本文件適用於微軟公司所發行之Windows 10作業系統。

## 項數統計

政府組態基準針對電腦作業環境提供一致性安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Windows 10組態基準計有381項設定項目，項目統計詳見表1，設定項目異動情形詳見附件1。

1. Windows 10組態基準項目統計

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 類別 | 項數 | 合計 |
| 1 | Windows10 Account Settings | 9 | 381 |
| 2 | Windows10 Computer Settings | 325 |
| 3 | Windows10 User Settings | 14 |
| 4 | Windows10 Firewall Settings | 33 |
| 本中心整理 | | | | |

## 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<https://www.nccst.nat.gov.tw/GCB>。

# Windows 10政府組態基準列表

1. Windows 10政府組態基準列表

| 項次 | GPO | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB 設定值 | 備註 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Windows10 Account Settings | TWGCB-01-005-0001 | 帳戶原則\密碼原則 | 密碼最短使用期限 | * 此項原則設定決定在使用者變更密碼之前，密碼必須使用的期限(天數)。可以設定1與998天之間的值，或設定天數為0，以允許立即變更 * 「密碼最短使用期限」不得超過「密碼最長使用期限」，除非「密碼最長使用期限」設定為0，表示密碼永遠不會到期。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以設定為介於0到998之間的任何數值 * 如果要讓「強制執行密碼歷程記錄」生效，請將「密碼最短使用期限」設為0以上 * 若沒有設定「密碼最短使用期限」，使用者便可重複使用密碼，直到厭倦為止。預設值並未依循此建議，所以系統管理員可為使用者指定密碼，然後在使用者登入時要求變更系統管理員定義的密碼。如果「密碼歷程記錄」設為0，使用者便不需選擇新密碼。因此，根據預設，「強制執行密碼歷程記錄」設定為1 | 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 | 1 天 | CCE-ID：CCE-41953-1 |
| 2 | Windows10 Account Settings | TWGCB-01-005-0002 | 帳戶原則\密碼原則 | 密碼最長使用期限 | * 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在1至999天之後到期；或將天數設為0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於1到999天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以是介於0到998天之間的任何數值 * 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每30至90天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限 * 注意：若使用者帳戶啟用「密碼永久有效」設定，將覆蓋此原則設定，導致系統不會要求該使用者變更密碼，即該使用者帳戶之密碼永遠不會到期 | 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 | 90天以下，但須大於0天 | CCE-ID：CCE-43535-4 |
| 3 | Windows10 Account Settings | TWGCB-01-005-0003 | 帳戶原則\密碼原則 | 最小密碼長度 | * 此項原則設定決定使用者帳戶的密碼可包含的最少字元數 * 此設定的最大值取決於「放寬最小密碼長度限制」的設定值 * 如果未定義「放寬最小密碼長度限制」設定，則此設定可以設為0到14 * 如果已定義並停用「放寬最小密碼長度限制」設定，則此設定可以設為0到14 * 如果已定義並啟用「放寬最小密碼長度限制」設定，則此設定可以設為0到128 * 將字元數設為0，則表示不需要密碼 | 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 | 8個字元以上 | CCE-ID：CCE-41679-2 |
| 4 | Windows10 Account Settings | TWGCB-01-005-0004 | 帳戶原則\密碼原則 | 密碼必須符合複雜性需求 | * 此項原則設定決定密碼是否必須符合複雜性需求 * 如果啟用了此原則，則密碼必須符合下列最小需求：   + 不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元   + 長度至少為6個字元   + 包含下列四種字元中的三種：  1. 英文大寫字元(A到Z) 2. 英文小寫字元(a到z) 3. 10進位數字(0到9) 4. 非英文字母字元(例如：!、$、#、%)  * 建立或變更密碼時會強制執行複雜性需求 | 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 | 啟用 | CCE-ID：CCE-42872-2 |
| 5 | Windows10 Account Settings | TWGCB-01-005-0005 | 帳戶原則\密碼原則 | 強制執行密碼歷程記錄 | * 此項原則設定決定重複使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於0與24個密碼之間 * 此項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性 | 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 | 3個以上記憶的密碼 | CCE-ID：CCE-42136-2 |
| 6 | Windows10 Account Settings | TWGCB-01-005-0006 | 帳戶原則\密碼原則 | 使用可還原的加密來存放密碼 | * 此項原則設定決定作業系統是否使用可還原的加密來存放密碼 * 此原則支援應用程式使用需要知道使用者密碼來進行驗證的通訊協定 * 使用可還原的加密來存放密碼，基本上與存放純文字密碼是相同的。基於這個理由，除非應用程式需求比保護密碼資訊重要，否則絕不應該啟用此項原則 * 當透過遠端存取或網際網路驗證服務(IAS)使用Challenge-Handshake驗證通訊協定進行驗證時，便需要此項原則。在網際網路資訊服務(IIS)中使用摘要式驗證時，也需要此項原則 | 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 | 停用 | CCE-ID：CCE-43536-2 |
| 7 | Windows10 Account Settings | TWGCB-01-005-0007 | 帳戶原則\帳戶原則 | 帳戶鎖定閾值 | * 此項原則設定決定使用者帳戶被鎖定的嘗試登入失敗次數，除非由系統管理員重設或該帳戶的鎖定期間已到期，否則無法使用該鎖定帳戶 * 可將失敗的登入嘗試值設定為介於0到999之間。如果將值設定為0，將永遠不會鎖定該帳戶 * 針對使用CTRL+ALT+DELETE或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾值 | 5次以下不正確的登入嘗試，但須大於0次 | CCE-ID：CCE-43894-5 |
| 8 | Windows10 Account Settings | TWGCB-01-005-0008 | 帳戶原則\帳戶原則 | 重設帳戶鎖定計數器的時間間隔 | * 此項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入嘗試計數器重設為0次失敗。可用的範圍是從1分鐘到99,999分鐘 * 如果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 | 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 | 15分鐘以上 | CCE-ID：CCE-42778-1 |
| 9 | Windows10 Account Settings | TWGCB-01-005-0009 | 帳戶原則\帳戶原則 | 帳戶鎖定期間 | * 此項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數 * 設定範圍從0分鐘到99,999分鐘。如果將帳戶鎖定期間設定為0，將會繼續鎖定帳戶，直到系統管理員將該帳戶解除鎖定 * 如果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 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定期間 | 15分鐘以上 | CCE-ID：CCE-43748-3 |
| 10 | Windows10 Computer Settings | TWGCB-01-005-0010 | 控制台\個人化 | 防止啟用鎖定畫面相機 | * 停用「電腦設定」中鎖定畫面相機切換開關，防止在鎖定畫面上叫用相機 * 根據預設，使用者可以啟用在鎖定畫面上叫用可用的相機 * 如果啟用此項設定，使用者將無法啟用或停用「電腦設定」中鎖定畫面相機存取，而且在鎖定畫面上不能叫用相機 | 電腦設定\系統管理範本\控制台\個人化\防止啟用鎖定畫面相機 | 啟用 | CCE-ID：CCE-43964-6 |
| 11 | Windows10 Computer Settings | TWGCB-01-005-0011 | 控制台\個人化 | 防止啟用鎖定畫面投影片放映 | * 停用「電腦設定」中鎖定畫面投影片放映設定，防止在鎖定畫面上播放投影片放映 * 根據預設，使用者可以啟用鎖定電腦後將要執行的投影片放映 * 如果啟用此項設定，使用者將無法修改「電腦設定」中投影片放映設定，也不會開始任何投影片放映 | 電腦設定\系統管理範本\控制台\個人化\防止啟用鎖定畫面投影片放映 | 啟用 | CCE-ID：CCE-42777-3 |
| 12 | Windows10 Computer Settings | TWGCB-01-005-0012 | 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 | * 此項原則設定決定是否要求網域使用者在設定網路的位置時必須提升權限 * 如果啟用此項原則設定，網域使用者在設定網路的位置時必須提升權限 * 如果停用或未設定此項原則設定，則網域使用者不必提升權限就可以設定網路的位置 | 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 | 啟用 | CCE-ID：CCE-41685-9 |
| 13 | Windows10 Computer Settings | TWGCB-01-005-0013 | 網路\網路連線 | 禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | * 此項原則設定決定使用者是否可以安裝及設定網路橋接器 * 注意：此項設定與位置有關。只有當電腦連線到相同DNS網域網路，而且在這個連線上更新設定，才會套用此項設定。如果設定更新之後，電腦又連線到其他不同的DNS網域網路，此項設定將不會生效 * 網路橋接器可以讓使用者建立層級2MAC橋接器，啟用橋接器可以將兩個(含)以上的網路區段連在一起。這個連線會出現在「網路連線」資料夾中 * 如果停用或未設定此項原則設定，則使用者可以建立並修改網路橋接器的設定。啟用此原則設定並不會從使用者的電腦移除現存的網路橋接器 | 電腦設定\系統管理範本\網路\網路連線\禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | 啟用 | CCE-ID：CCE-42392-1 |
| 14 | Windows10 Computer Settings | TWGCB-01-005-0014 | 網路\網路連線 | 透過內部網路路由傳送所有流量 | * 此項原則設定會決定遠端用戶端電腦會透過內部網路來路由傳送網際網路流量，或是由用戶端直接存取網際網路 * 當遠端用戶端電腦使用Direct Access連線到內部網路時，它可以用兩種方式存取網際網路，透過Direct Access在電腦與內部網路之間建立的安全通道，或是直接透過本機預設閘道器 * 如果啟用此項原則設定，執行Direct Access的遠端用戶端電腦與網際網路之間的所有流量會透過內部網路路由傳送 * 如果停用此項原則設定，執行Direct Access的遠端用戶端電腦與網際網路之間的流量不會透過內部網路路由傳送 * 如果未設定此項原則設定，則執行Direct Access的遠端用戶端電腦與網際網路之間的流量不會透過內部網路路由傳送 | 電腦設定\系統管理範本\網路\網路連線\透過內部網路路由傳送所有流量 | 啟用 | CCE-ID：CCE-42058-8 |
| 15 | Windows10 Computer Settings | TWGCB-01-005-0015 | 網路\網路提供者 | 已強化的UNC路徑 | * 此原則設定可設定UNC路徑的安全存取 * 若啟用此原則，在滿足額外的安全性需求之後，Windows只會允許對所指定UNC路徑的存取 | 電腦設定\系統管理範本\網路\網路提供者\已強化的UNC路徑 | 啟用，  Value Name: \\\*\SYSVOL  Value: RequireMutualAuthentication=1, RequireIntegrity=1  Value Name: \\\*\NETLOGON  Value: RequireMutualAuthentication=1, RequireIntegrity=1 | CCE-ID：CCE-42497-8 |
| 16 | Windows10 Computer Settings | TWGCB-01-005-0016 | 網路\Windows連線管理員 | 最小化網際網路或Windows網域的同時連線數目 | * 此項原則設定會決定電腦是否能對網際網路或Windows網域有多個連線。若允許多個連線，則會接著決定網路流量的路由方式 * 若此項原則設定設為「0=允許同時連線」，電腦就能對網際網路、Windows網域或兩者具有同時連線。網際網路流量可透過所有連線路由，包括行動數據連線和所有計量付費網路。這在此項原則設定原本處於「已停用」狀態 * 若此項原則設定設為「1=將同時連線最小化」，則會在電腦對慣用類型的網路至少有一個正在使用的網際網路連線時，封鎖所有新的自動化網際網路連線。此為慣用類型的順序(從最慣用至最不慣用排序)：乙太網路>WLAN>行動數據。乙太網路一律是慣用的連線類型，但使用者仍可手動連線至任何網路。這在此項原則設定中原本處於「已啟用」狀態 * 若此項原則設定設為「2=保持行動數據的連線」，則行為會與1相似。不過，若有行動數據連線可用，則會為需要行動數據連線的服務一律保持連線。當使用者連線至WLAN或乙太網路連線時，不會透過行動數據連線路由任何網際網路流量。此選項最早於Windows 10(1703版)提供使用 * 若此項原則設定設為「3=使用乙太網路時禁止Wi-Fi」，則行為會與2相似。不過，若存在乙太網路連線，Windows就不會允許使用者手動連線至WLAN。只有不存在乙太網路連線時才能連線(自動或手動)至WLAN | 電腦設定\系統管理範本\網路\Windows連線管理員\最小化網際網路或Windows網域的同時連線數目 | 啟用：3=使用乙太網路時禁止Wi-Fi | CCE-ID：CCE-41857-4 |
| 17 | Windows10 Computer Settings | TWGCB-01-005-0017 | 網路\Windows連線管理員 | 當連線到通過網域驗證的網路時，禁止連線到非網域網路 | * 此項原則設定可避免電腦同時連線到網域型網路以及非網域型網路 * 如果啟用此項原則設定，電腦會依據下列情況，回應自動及手動網路連線嘗試：   + 自動連線嘗試  1. 當電腦已經連線到網域型網路時，會封鎖連線到非網域型網路的所有自動連線嘗試 2. 當電腦已經連線到非網域型網路時，會封鎖連線到網域型網路的自動連線嘗試    * 手動連線嘗試 3. 當電腦已經透過非乙太網路的媒體連線到非網域型網路或網域型網路，而且使用者嘗試違反此項原則設定來建立連線到其他網路的手動連線時，會中斷現有的網路連線，而允許手動連線 4. 當電腦已經透過乙太網路連線到非網域型網路或網域型網路，而且使用者嘗試違反此項原則設定來建立連線到其他網路的手動連線時，會維持現有的乙太網路連線，而封鎖手動連線嘗試 | 電腦設定\系統管理範本\網路\Windows連線管理員\當連線到通過網域驗證的網路時，禁止連線到非網域網路 | 啟用 | CCE-ID：CCE-43419-1 |
| 18 | Windows10 Computer Settings | TWGCB-01-005-0018 | 網路\連結階層拓樸搜索 | 開啟Mapper I/O(LLTDIO)驅動程式 | * 此項原則設定會變更Mapper I/O網路通訊協定驅動程式的操作行為 * LLTDIO允許電腦搜索其連線網路的拓撲。也允許電腦起始服務品質(Quality-of-Service)要求，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，使用者可以使用其他選項來微調選取項目，可以選擇「允許在網域中操作」選項，以允許LLTDIO在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，使用者就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用LLTDIO的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟Mapper I/O(LLTDIO)驅動程式 | 停用 | CCE-ID：CCE-43138-7 |
| 19 | Windows10 Computer Settings | TWGCB-01-005-0019 | 網路\連結階層拓樸搜索 | 開啟Responder(RSPNDR)驅動程式 | * 此項原則設定決定是否變更Responder網路通訊協定驅動程式的操作行為 * Responder允許電腦加入「連結階層拓樸搜索」要求，以便能在網路上搜索並找到該電腦。也允許電腦加入服務品質(Quality-of-Service)活動，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，則可以使用其他選項來微調選取項目。若選擇「允許在網域中操作」選項，以允許Responder在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用Responder的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟Responder(RSPNDR)驅動程式 | 停用 | CCE-ID：CCE-42028-1 |
| 20 | Windows10 Computer Settings | TWGCB-01-005-0020 | 網路\Lanman工作站 | 啟用不安全的來賓登入 | * 此原則設定可決定SMB用戶端是否允許以不安全的來賓身分登入SMB伺服器 * 若啟用此原則設定或未設定此原則設定，SMB用戶端將允許不安全的來賓登入 * 若停用此原則設定，SMB用戶端將拒絕不安全的來賓登入 * 檔案伺服器使用不安全的來賓登入來允許共用資料夾的未經驗證存取，雖然在機關環境中不常見，做為檔案伺服器的消費性「網路連接儲存裝置」(NAS)設備經常使用不安全的來賓登入。Windows檔案伺服器需要驗證，而且預設不會使用不安全的來賓登入。因為不安全的來賓登入未經驗證，重要安全性功能(例如「SMB簽署」與「SMB加密」)會被停用。因此，允許不安全的來賓登入之用戶端容易遭受各種攔截式攻擊，進而導致資料遺失、資料損毀與暴露於惡意程式碼。此外，使用不安全的來賓登入方式寫入到檔案伺服器的所有資料可能可供網路上的任何人存取 | 電腦設定\系統管理範本\網路\Lanman工作站\啟用不安全的來賓登入 | 停用 | CCE-ID：CCE-44419-0 |
| 21 | Windows10 Computer Settings | TWGCB-01-005-0021 | 網路\Microsoft對等網路服務 | 關閉Microsoft對等網路服務 | * 此項原則設定決定是否關閉Microsoft對等網路服務，並導致所有依存的應用程式停止運作 * 對等通訊協定允許RTC、協同作業、內容發布和分散式處理等領域的應用程式 * 如果啟用此原則設定，將會關閉對等通訊協定 * 如果停用或未設定此原則設定，將會開啟對等通訊協定 | 電腦設定\系統管理範本\網路\Microsoft對等網路服務\關閉Microsoft對等網路服務 | 啟用 | CCE-ID：CCE-43162-7 |
| 22 | Windows10 Computer Settings | TWGCB-01-005-0022 | 網路\TCPIP設定值\IPv6轉換技術 | 設定6to4狀態 | * 此項原則設定可設定6to4，這個位址指派以及路由器對路由器自動通道技術是用來提供IPv4網際網路上IPv6站台與主機之間的單點傳播IPv6連線。6to4使用全域位址首碼：2002：WWXX：YYZZ：：/48，其中英文字母是指派給站台的全域IPv4位址(w.x.y.z)的十六進位表示 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，可在6to4指定以下其中一項設定：   + 預設狀態：如果主機只有連結本機IPv6的上網能力以及公用的IPv4位址，則會啟用6to4。如果沒有全域IPv6位址，也沒有全域IPv4位址，主機將沒有6to4介面。如果沒有全域IPv6位址，但是有全域IPv4位址，主機將有6to4介面   + 啟用狀態：如果有全域IPv4位址，主機將有6to4介面。如果沒有全域IPv4位址，主機將沒有6to4介面   + 停用狀態：6to4為關閉狀態，而且無法使用與6to4的連線 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定6to4狀態 | 啟用 | CCE-ID：CCE-43439-9 |
| 23 | Windows10 Computer Settings | TWGCB-01-005-0023 | 網路\TCPIP設定值\IPv6轉換技術 | 設定IP-HTTPS狀態 | * 此項原則設定可讓使用者設定IP-HTTPS，這個通道技術使用HTTPS通訊協定提供遠端網路的IP連線 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，則可以指定IP-HTTPS伺服器URL。可以下列其中一個設定來設定IP-HTTPS：   + 預設狀態：沒有其他連線選項時即使用IP-HTTPS介面   + 啟用狀態：即使主機有其他連線介面，仍會一直提供IP-HTTPS介面   + 停用狀態：主機不提供IP-HTTPS介面 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定IP-HTTPS狀態 | 啟用，  輸入IPHTTPS URL：http：//localhost 從下列選項中選取介面狀態：停用狀態 | CCE-ID：CCE-44105-5 |
| 24 | Windows10 Computer Settings | TWGCB-01-005-0024 | 網路\TCPIP設定值\IPv6轉換技術 | 設定ISATAP狀態 | * 此項原則設定可設定「內部網站自動通道定址通訊協定」(Intra-Site Automatic Tunnel Addressing Protocol, ISATAP)，這個位址對路由器、主機對主機、主機對路由器，以及路由器對主機的自動通道技術是用來提供IPv4內部網站上各IPv6主機間的單點傳播IPv6連線 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，可以下列其中一個設定來設定ISATAP：   + 預設狀態：如果成功解析ISATAP路由器名稱，主機會為ISATAP設定一個連結本機位址，並透過無狀態位址自動設定，為ISATAP路由器收到的每個首碼設定一個位址。如果無法成功解析ISATAP路由器名稱，則無法在使用對應IPv4位址的主機上使用ISATAP連線   + 啟用狀態：如果成功解析ISATAP名稱，主機會為ISATAP設定一個連結本機位址，並透過無狀態位址自動設定，為ISATAP路由器收到的每個首碼設定一個位址。如果無法成功解析ISATAP名稱，主機會用連結本機位址來設定ISATAP介面   + 停用狀態：主機不提供ISATAP介面 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定ISATAP狀態 | 啟用 | CCE-ID：CCE-43061-1 |
| 25 | Windows10 Computer Settings | TWGCB-01-005-0025 | 網路\TCPIP設定值\IPv6轉換技術 | 設定Teredo狀態 | * 此項原則設定可讓使用者設定Teredo，它是在IPv4網際網路上提供單點傳播IPv6連線的位址指派與自動通道技術 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，可用下列其中一個設定來設定Teredo：   + 預設狀態：預設狀態是「用戶端」   + 停用狀態：主機不提供Teredo介面   + 用戶端：只有當主機不是位在包含網域控制站的網路時，才提供Teredo介面   + 企業版用戶端：即使主機位在包含網域控制站的網路上，也會提供Teredo介面 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定Teredo狀態 | 啟用 | CCE-ID：CCE-42793-0 |
| 26 | Windows10 Computer Settings | TWGCB-01-005-0026 | 網路\Windows Connect Now | 使用Windows Connect Now進行無線設定 | * 此項原則設定允許使用Windows Connect Now(WCN)進行無線設定。WCN登錄器可經由Windows可攜式裝置(WPD)與USB快閃磁碟機，來尋找和設定Ethernet(UPnP)與In-band 802.11 Wi-Fi上的裝置，其他選項則允許在指定的媒體上進行搜索與設定 * 如果啟用此項原則設定，就有額外選項可以關閉特定媒體上的操作 * 如果停用此項原則設定，將會停用所有媒體上的操作 * 如果未設定此項原則設定，將會啟用所有媒體上的操作。此原則設定的預設值可允許所有媒體上的操作 | 電腦設定\系統設定範本\網路\Windows Connect Now\使用Windows Connect Now進行無線設定 | 停用 | CCE-ID：CCE-43024-9 |
| 27 | Windows10 Computer Settings | TWGCB-01-005-0027 | 網路\Windows Connect Now | 禁止存取Windows Connect Now精靈 | * 這項原則設定決定是否禁止對Windows Connect Now(WCN)精靈的存取 * 如果啟用這項原則設定，就會停用精靈，而使用者會無法存取任何精靈工作。所有和設定相關的工作，包含「設定無線路由器或存取點」與「新增無線裝置」都會被停用 * 如果停用或不設定此原則，使用者將可存取精靈工作；包含「設定無線路由器或存取點」與「新增無線裝置」。根據預設，這項原則設定會允許使用者存取所有的WCN精靈 | 電腦設定\系統管理範本\網路\Windows Connect Now\禁止存取Windows Connect Now精靈 | 啟用 | CCE-ID：CCE-42952-2 |
| 28 | Windows10 Computer Settings | TWGCB-01-005-0028 | 網路\WLAN服務 | 允許Windows自動連線到建議的開放式熱點、連絡人分享的網路或提供付費服務的熱點 | * 此項原則設定可決定使用者是否可以啟用WLAN設定「連線到建議的開放式熱點」、「連線到我的連絡人分享的網路」與「啟用付費服務」 * 「連線到建議的開放式熱點」可讓Windows自動將使用者連線到開放式熱點(透過其他使用者使用Windows連線的群眾外包網路所得知) * 「連線到我的連絡人分享的網路」可讓Windows自動連線到使用者的連絡人所分享的網路，並讓此裝置上的使用者與其連絡人分享網路 * 「啟用付費服務」可讓Windows暫時連線到開放式熱點，以判斷是否有可用的付費服務 * 若停用此原則設定，將同時關閉「連線到建議的開放式熱點」、「連線到我的連絡人分享的網路」與「啟用付費服務」，且此裝置上的使用者將無法啟用它們 | 電腦設定\系統管理範本\網路\WLAN服務\WLAN設定\允許Windows自動連線到建議的開放式熱點、連絡人分享的網路或提供付費服務的熱點 | 停用 | CCE-ID：CCE-42544-7 |
| 29 | Windows10 Computer Settings | TWGCB-01-005-0029 | 系統\稽核建立處理程序 | 在建立處理程序事件中包含命令列 | * 此項原則設定可決定建立新的處理程序之後，要將哪些資訊記錄到安全性稽核事件中 * 必須啟用「稽核建立處理程序」原則後才能套用此項設定。如果啟用此項原則設定，每個處理程序的命令列資訊會以純文字形式記錄到安全性事件記錄中，做為套用此原則設定之工作站和伺服器上稽核建立處理程序事件4688「已建立新的處理程序」的一部分 * 如果停用或未設定此項原則設定，處理程序的命令列資訊將不會包含在稽核建立處理程序事件中 * 注意：如果啟用此項原則設定，具有讀取安全性事件存取權的任何使用者，將能夠讀取任何成功建立的處理程序的命令列引數。命令列引數可以包含敏感或私人資訊，如密碼或使用者資料 | 電腦設定\系統管理範本\系統\稽核建立處理程序\在建立處理程序事件中包含命令列 | 停用 | CCE-ID：CCE-43923-2 |
| 30 | Windows10 Computer Settings | TWGCB-01-005-0030 | 系統\裝置安裝 | 防止從網際網路擷取裝置中繼資料 | * 此項原則設定決定是否防止Windows從網際網路擷取裝置中繼資料 * 如果啟用此項原則設定，Windows不會從網際網路為安裝的裝置擷取裝置中繼資料。此項原則設定會覆寫「裝置安裝設定」對話方塊(「控制台」>「系統及安全性」>「系統」>「進階系統設定」>「硬體」索引標籤)中的設定 * 如果停用或未設定此項原則設定，則由「裝置安裝設定」對話方塊中的設定控制Windows是否會從網際網路擷取裝置中繼資料 | 電腦設定\系統管理範本\系統\裝置安裝\防止從網際網路擷取裝置中繼資料 | 啟用 | CCE-ID：CCE-42758-3 |
| 31 | Windows10 Computer Settings | TWGCB-01-005-0031 | 系統\開機初期啟動的反惡意程式碼 | 開機啟動驅動程式初始化原則 | * 此項原則設定允許使用者根據開機初期啟動的反惡意程式碼開機啟動驅動程式所判斷的分類，指定要初始化哪些開機啟動驅動程式。開機初期啟動的反惡意程式碼開機啟動驅動程式可以針對每個開機啟動驅動程式傳回下列分類：   + 良好：驅動程式已經過簽署，且未遭竄改   + 不良：驅動程式已被識別為惡意程式碼。建議使用者不要初始化已知的不良驅動程式   + 不良但關鍵：驅動程式已被識別為惡意程式碼，但電腦必須載入此驅動程式才能成功開機   + 不明：此驅動程式尚未經由使用者的惡意程式碼偵測應用程式保證，也尚未經由開機初期啟動的反惡意程式碼開機啟動驅動程式分類 * 如果啟用此項原則設定，使用者可以選擇下次電腦啟動時要初始的啟動開機驅動程式 * 如果停用或未設定此項原則設定，便會初始化判斷為「良好」、「不明」或「不良但關鍵」的開機啟動驅動程式，但不會初始判斷為「不良」的驅動程式 * 如果惡意程式碼偵測應用程式不含開機初期啟動的反惡意程式碼開機啟動驅動程式，或如果已停用使用者的開機初期啟動的反惡意程式碼開機啟動驅動程式，則此項設定便不會發生作用，系統會初始化所有的開機啟動驅動程式 | 電腦設定\系統管理範本\系統\開機初期啟動的反惡意程式碼\開機啟動驅動程式初始化原則 | 啟用，良好和不明 | CCE-ID：CCE-43463-9 |
| 32 | Windows10 Computer Settings | TWGCB-01-005-0032 | 系統\群組原則 | 設定登錄原則處理 | * 此項原則設定可決定更新登錄原則的時間，此設定會影響「系統管理範本」資料夾中的所有原則，以及在登錄中儲存值的任何其他原則，它會覆蓋當初安裝程式時，該程式所執行的登錄原則組的自訂設定 * 如果啟用此項原則設定，可以使用所提供的核取方塊來變更選項 * 如果停用此項原則或不加以設定，則在系統上就不會產生作用 * 「在定期的背景處理期間不要套用」選項會禁止系統在電腦使用中，對受到影響的原則進行背景更新。停用背景更新後，要等到下一個使用者登入或重新啟動系統時，原則變更才會生效 * 「即使群組原則物件尚未變更也進行處理」選項會更新並重新套用原則。許多原則會指定只有在原則變更後，才進行更新 | 電腦設定\系統管理範本\系統\群組原則\設定登錄原則處理 | 啟用，即使群組原則物件尚未變更也進行處理 | CCE-ID：CCE-41701-4 |
| 33 | Windows10 Computer Settings | TWGCB-01-005-0033 | 系統\登入 | 不要顯示網路選取UI | * 此項原則設定可控制是否讓任何人在登入畫面上與可用的網路UI互動 * 如果啟用此項原則設定，則登入Windows之後才能變更電腦的網路連線狀態 * 如果停用或未設定此項原則設定，任何人不用登入Windows就可以中斷電腦與網路的連線或將電腦連線到其他可用的網路 | 電腦設定\系統管理範本\系統\登入\不要顯示網路選取UI | 啟用 | CCE-ID：CCE-43993-5 |
| 34 | Windows10 Computer Settings | TWGCB-01-005-0034 | 系統\登入 | 不要列舉加入網域電腦上的連線使用者 | * 此項原則設定會禁止列舉加入網域電腦上的連線使用者 * 如果啟用此項原則設定，登入介面不會列舉加入網域電腦上的連線使用者 * 如果停用或未設定此項原則設定，則會列舉加入網域電腦上的連線使用者 | 電腦設定\系統管理範本\系統\登入\不要列舉加入網域電腦上的連線使用者 | 啟用 | CCE-ID：CCE-44126-1 |
| 35 | Windows10 Computer Settings | TWGCB-01-005-0035 | 系統\登入 | 不要處理只執行一次清單 | * 此項原則設定會忽略自訂的執行一次清單 * 使用者可以建立一份系統在下次啟動時會自動啟動(但之後就不再自動啟動)的自訂額外程式與文件清單。這些程式會加入由系統啟動的程式與服務標準清單中 * 如果啟用此項原則設定，則系統會略過執行一次清單 * 如果停用或未設定此項原則設定，系統會執行只執行一次清單中的程式 * 此項原則設定會同時出現在「電腦設定」與「使用者設定」資料夾中。如果同時設定這兩個原則設定，則「電腦設定」中的原則設定將優先於「使用者設定」中的原則設定 * 注意：自訂的只執行一次清單存放在HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce的登錄中 | 電腦設定\系統管理範本\系統\登入\不要處理只執行一次清單 | 啟用 | CCE-ID：CCE-44292-1 |
| 36 | Windows10 Computer Settings | TWGCB-01-005-0036 | 系統\登入 | 列舉加入網域電腦上的本機使用者 | * 此項原則設定會允許列舉加入網域電腦上的本機使用者 * 如果啟用此項原則設定，登入介面將會列舉加入網域電腦上的本機使用者 * 如果停用或未設定此項原則設定，則登入介面將不會列舉加入網域電腦上的連線使用者 | 電腦設定\系統管理範本\系統\登入\列舉加入網域電腦上的本機使用者 | 停用 | CCE-ID：CCE-43551-1 |
| 37 | Windows10 Computer Settings | TWGCB-01-005-0037 | 系統\登入 | 關閉鎖定畫面上的應用程式通知 | * 此項原則設定可以讓使用者不要在鎖定畫面上顯示應用程式通知 * 如果啟用該原則設定，則不會在鎖定畫面上顯示應用程式通知 * 如果停用或未設定此項原則設定，則使用者可以選擇要在鎖定畫面上顯示通知的應用程式 | 電腦設定\系統管理範本\系統\登入\關閉鎖定畫面上的應用程式通知 | 啟用 | CCE-ID：CCE-42172-7 |
| 38 | Windows10 Computer Settings | TWGCB-01-005-0038 | 系統\登入 | 開啟方便的PIN登入 | * 此項原則設定可以讓使用者控制是否讓網域使用者使用方便的PIN登入 * 如果啟用此項原則設定，網域使用者可以設定並使用方便的PIN登入 * 如果停用或未設定此項原則設定，則網域使用者無法設定並使用方便的PIN * 請注意，使用這個功能時，使用者的網域密碼會在系統保存庫中快取 | 電腦設定\系統管理範本\系統\登入\開啟方便的PIN登入 | 停用 | CCE-ID：CCE-44437-2 |
| 39 | Windows10 Computer Settings | TWGCB-01-005-0039 | 系統\登入 | 永遠使用傳統登入 | * 此項原則設定決定是否強制使用者使用傳統登入畫面來登入電腦 * 預設狀況下，工作群組是設定成使用簡單登入畫面 * 此項設定只能在電腦未加入網域時使用 | 電腦設定\系統管理範本\系統\登入\永遠使用傳統登入 | 啟用 | CCE-ID：CCE-42429-1 |
| 40 | Windows10 Computer Settings | TWGCB-01-005-0040 | 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) | * 此項原則設定決定使用電池時，系統從睡眠狀態中恢復時，是否會提示使用者輸入密碼 * 如果啟用或未設定此原則，當系統從睡眠狀態中恢復時，就會提示使用者輸入密碼 * 如果停用此原則，當系統從睡眠狀態中恢復時，就不會提示使用者輸入密碼 | 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) | 啟用 | CCE-ID：CCE-44052-9 |
| 41 | Windows10 Computer Settings | TWGCB-01-005-0041 | 系統\電源管理\睡眠設定 | 喚醒電腦時必須使用密碼(一般電源) | * 此項原則設定決定使用一般電源時，系統從睡眠狀態中恢復時，是否會提示使用者輸入密碼 * 如果啟用或未設定此原則，當系統從睡眠狀態中恢復時，就會提示使用者輸入密碼 * 如果停用此原則，當系統從睡眠狀態中恢復時，就不會提示使用者輸入密碼 | 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(一般電源) | 啟用 | CCE-ID：CCE-41676-8 |
| 42 | Windows10 Computer Settings | TWGCB-01-005-0042 | 系統\遠端協助 | 設定提供遠端協助 | * 此項原則設定可在這部電腦上開啟或關閉「提供(未經要求)遠端協助」 * 如果啟用此項原則設定，這部電腦上的使用者可使用「提供(未經要求)遠端協助」，從機關的技術支援團隊取得協助 * 如果停用或未設定此項原則設定，這部電腦上的使用者無法使用「提供(未經要求)遠端協助」，從機關的技術支援團隊取得協助 * 如果啟用此項原則設定，有兩種方法可以讓協助人員提供遠端協助：「只允許協助人員檢視電腦」或「允許協助人員從遠端控制電腦」。設定此項原則設定時，也同時指定了允許提供遠端協助的使用者或使用者群組清單 * 如果要設定協助人員清單，請按一下「顯示」。在開啟的視窗中，輸入協助人員的名稱。請逐一加入使用者或群組。輸入協助人員的使用者名稱或使用者群組名稱時，請使用下列格式： <網域名稱>\<使用者名稱>或 <網域名稱>\<群組名稱> * 如果啟用此項原則設定，使用者也應該啟用防火牆例外，以允許遠端協助通訊。「提供(未經要求)遠端協助」所需的防火牆例外視執行中的Windows版本而定   + Windows Vista和更新版本：   啟用網域設定檔的遠端協助例外。例外必須包含：  Port135：TCP %WINDIR%\System32\msra.exe %WINDIR%\System32\raserver.exe | 電腦設定\系統管理範本\系統\遠端協助\設定提供遠端協助 | 停用 | CCE-ID：CCE-42975-3 |
| 43 | Windows10 Computer Settings | TWGCB-01-005-0043 | 系統\遠端協助 | 設定請求遠端協助 | * 此項原則設定可以讓使用者在這部電腦上開啟或關閉「請求(要求)遠端協助」 * 如果啟用該原則設定，這部電腦上的使用者即可使用電子郵件或檔案傳輸來要求他人協助。此外，使用者可以使用立即訊息程式，讓他人可以連線到這部電腦，使用者也可以設定其他遠端協助設定 * 如果停用此項原則設定，這部電腦上的使用者無法使用電子郵件或檔案傳輸來要求他人協助。此外，使用者無法使用立即訊息程式允許他人連線到這部電腦 * 如果使用者未設定此項原則設定，使用者可以在「控制台」的「系統內容」中自行開啟或關閉「請求(要求)遠端協助」。使用者也可以設定遠端協助設定 * 如果啟用此項原則設定，有兩種方法可以讓協助人員提供遠端協助：「只允許協助人員檢視電腦」或「允許協助人員從遠端控制電腦」 * 「票證時間最大值」原則設定可設定使用電子郵件或檔案傳輸所建立的遠端協助邀請可維持開啟的時間限制 * 「選擇傳送電子郵件邀請的方法」設定可指定傳送遠端協助邀請時，要使用何種電子郵件標準。視電子郵件程式而定，可以使用Mailto標準(透過網際網路連結連接的邀請收件者)或SMAPI(SimpleMAPI)標準(附加至電子郵件訊息的邀請) * 如果啟用此項原則設定，也應該啟用適當的防火牆例外，以允許遠端協助通訊 | 電腦設定\系統管理範本\系統\遠端協助\設定請求遠端協助 | 停用 | CCE-ID：CCE-42852-4 |
| 44 | Windows10 Computer Settings | TWGCB-01-005-0044 | 系統\遠端協助 | 開啟工作階段記錄 | * 此項原則設定可讓使用者開啟或關閉記錄。記錄檔位於使用者之「遠端協助」下的「文件」資料夾中 * 如果啟用此項原則設定，就會產生記錄檔 * 如果停用此項原則設定，就不會產生記錄檔 * 如果未設定此項原則設定，就會使用以應用程式為基礎的設定 | 電腦設定\系統管理範本\系統\遠端協助\開啟工作階段記錄 | 啟用 | CCE-ID：CCE-41626-3 |
| 45 | Windows10 Computer Settings | TWGCB-01-005-0045 | 系統\遠端程序呼叫 | 啟用RPC端點對應程式用戶端驗證 | * 此項原則設定決定與端點對應程式服務進行通訊的RPC用戶端是否進行驗證 * 如果啟用此項原則設定，與端點對應程式服務進行通訊的RPC用戶端，只要即將解析端點的RPC呼叫具有授權資訊，就必須進行驗證 * 如果停用此項原則設定，與端點對應程式服務進行通訊的RPC用戶端將不進行驗證 * 注意：系統必須重新開機，才能套用此項原則 | 電腦設定\系統管理範本\系統\遠端程序呼叫\啟用RPC端點對應程式用戶端驗證 | 啟用 | CCE-ID：CCE-43456-3 |
| 46 | Windows10 Computer Settings | TWGCB-01-005-0046 | 系統\遠端程序呼叫 | 限制未經驗證的RPC用戶端 | * 此項原則設定控制RPC伺服器執行階段處理未經驗證的 RPC用戶端連線至RPC伺服器的方式 * 如果啟用此原則設定，它將會指示RPC執行階段限制未經驗證的RPC用戶端連線到電腦上執行的RPC伺服器。如果用戶端使用具名管道與伺服器進行通訊，或是使用RPC安全性，該用戶端就會被視為已驗證的用戶端。特別指定可以由未經驗證的用戶端存取的RPC介面有可能不受此限制，需視此原則的選取值而定 * 如果啟用此項原則設定，則可使用下列值：   + 無：允許所有RPC用戶端連線到已套用原則之電腦上所執行的RPC伺服器   + 已驗證：只允許已驗證的RPC用戶端(如上述定義)連線到已套用原則之電腦上所執行的RPC伺服器。已要求不受此限制的介面將得到豁免   + 已在無例外下驗證：只允許已驗證的RPC用戶端(如上述定義)連線到已套用原則之電腦上所執行的RPC伺服器。不允許例外 * 注意：系統必須重新開機，才能套用此原則設定 | 電腦設定\系統管理範本\系統\遠端程序呼叫\限制未經驗證的RPC用戶端 | 啟用，已驗證 | CCE-ID：CCE-43567-7 |
| 47 | Windows10 Computer Settings | TWGCB-01-005-0047 | 系統\裝置安裝 | 當裝置上已安裝標準驅動程式時，不要傳送Windows錯誤報告 | * 此項原則設定決定當裝置上已安裝標準驅動程式時，是否要傳送Windows錯誤報告 * 如果啟用此項原則設定，在已安裝標準驅動程式時，不會傳送Windows錯誤報告 * 如果停用或未設定此項原則設定，則在已安裝標準驅動程式時，會傳送Windows錯誤 | 電腦設定\系統管理範本\系統\裝置安裝\當裝置上已安裝標準驅動程式時，不要傳送Windows錯誤報告 | 啟用 | CCE-ID：CCE-41658-6 |
| 48 | Windows10 Computer Settings | TWGCB-01-005-0048 | 系統\裝置安裝 | 在通常會提示建立系統還原點的裝置活動期間，防止建立系統還原點 | * 此項原則設定決定是否在通常會提示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。在正常狀況下，Windows會為某些驅動程式活動(例如安裝未經簽署的驅動程式)建立還原點。系統還原點讓使用者能夠比較容易將系統還原到該活動之前的狀態 * 如果啟用此項原則設定，Windows不會在通常會建立系統還原點的時候建立系統還原點 * 如果停用或未設定此項原則設定，則Windows會依照正常方式建立系統還原點 | 電腦設定\系統管理範本\系統\裝置安裝\在通常會提示建立系統還原點的裝置活動期間，防止建立系統還原點 | 停用 | CCE-ID：CCE-41550-5 |
| 49 | Windows10 Computer Settings | TWGCB-01-005-0049 | 系統\裝置安裝 | 指定裝置驅動程式來源位置的搜尋順序 | * 此項原則設定決定是否指定Windows搜尋裝置驅動程式的來源位置時的搜尋順序 * 如果啟用此項原則設定，使用者可以選擇Windows在WindowsUpdate搜尋驅動程式為無條件搜尋、僅需要時搜尋或不搜尋 * 如果停用或未設定此項原則設定，則Administrators群組的成員可以決定Windows會依什麼順序搜尋裝置驅動程式的來源位置 | 電腦設定\系統管理範本\系統\裝置安裝\指定裝置驅動程式來源位置的搜尋順序 | 啟用，不搜尋Windows Update | CCE-ID：CCE-42345-9 |
| 50 | Windows10 Computer Settings | TWGCB-01-005-0050 | 系統\裝置安裝 | 允許遠端存取隨插即用介面 | * 此項原則設定決定是否允許遠端存取隨插即用介面 * 如果啟用此項原則設定，將允許從遠端連線到隨插即用介面 * 如果停用或未設定此項原則設定，則不允許從遠端連線到隨插即用介面 | 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 | 停用 | CCE-ID：CCE-43086-8 |
| 51 | Windows10 Computer Settings | TWGCB-01-005-0051 | 系統\疑難排解與診斷 | Microsoft支援服務診斷工具：開啟MSDT與支援提供者的互動式通訊 | * Microsoft支援服務診斷工具(MSDT)會蒐集診斷資料，供專業支援人員進行分析 * 如果啟用此項原則設定，使用者可以使用MSDT蒐集診斷資料，並傳送給專業支援人員，以解決問題，支援提供者預設為Microsoft Corporation * 如果停用此項原則設定，MSDT無法以支援模式執行，而且不會蒐集任何資料，或傳送給支援提供者 * 如果未設定此項原則設定，則預設啟用MSDT支援模式 * 此項原則不需重新開機或重新啟動服務就會生效，變更會立即生效 | 電腦設定\系統管理範本\系統\疑難排解與診斷\Microsoft支援服務診斷工具\Microsoft支援服務診斷工具：開啟MSDT與支援提供者的互動式通訊 | 停用 | CCE-ID：CCE-41770-9 |
| 52 | Windows10 Computer Settings | TWGCB-01-005-0052 | 系統\疑難排解與診斷 | 啟用/停用PrefTrack | * 此項原則設定決定要啟用或停用回應事件的追蹤 * 如果啟用此項原則設定，就會處理並彙總回應事件。彙總的資料會透過SQM傳到Microsoft * 如果停用此項原則設定，就不會處理回應事件 * 如果未設定此項原則設定，DPS會預設啟用Windows效能PerfTrack | 電腦設定\系統管理範本\系統\疑難排解與診斷\Windows效能PrefTrack\啟用/停用PrefTrack | 停用 | CCE-ID：CCE-44210-3 |
| 53 | Windows10 Computer Settings | TWGCB-01-005-0053 | 系統\疑難排解與診斷 | 疑難排解：允許使用者從「疑難排解控制台」存取Microsoft伺服器上的線上疑難排解內容(經由Windows線上疑難排解服務-WOTS) | * 此項原則設定可讓連線到網際網路的使用者存取和搜尋裝載在Microsoft內容伺服器上的疑難排解內容。使用者在「疑難排解控制台」UI中看到「您要取得可供疑難排解使用的最新內容嗎?」提示訊息時，只要按一下「是」，就可以存取線上疑難排解內容 * 如果啟用或未設定此項原則設定，連線到網際網路的使用者可以從「疑難排解控制台」使用者介面存取和搜尋裝載在Microsoft內容伺服器上的疑難排解內容 * 如果停用此項原則設定，則使用者即使已連線到網際網路，也只能存取和搜尋本機電腦上可用的疑難排解內容。他們無法連線到裝載Windows線上疑難排解服務的Microsoft伺服器 | 電腦設定\系統管理範本\系統\疑難排解與診斷\執行指令的診斷\疑難排解：允許使用者從「疑難排解控制台」存取Microsoft伺服器上的線上疑難排解內容(經由Windows線上疑難排解服務-WOTS) | 停用 | CCE-ID：CCE-42145-3 |
| 54 | Windows10 Computer Settings | TWGCB-01-005-0054 | 系統\Windows時間服務\時間提供者 | 設定Windows NTP用戶端 | * 此項原則設定決定是否指定用於控制Windows NTP用戶端的參數組 * 如果啟用此項原則設定，可以指定Windows NTP用戶端的下列參數 * 如果停用或未設定此項原則設定，Windows NTP用戶端會使用下列每個參數的預設值   + NtpServer：NTP時間來源的網域名稱系統(DNS)名稱或IP位址。這個值的格式為「dnsName，flags」，其中flags是該主機之旗標的十六進位位元遮罩，預設值是time.windows.com,0x09   + Type：這個值用於控制W32time使用的驗證方式。預設值是NT5DS   + CrossSiteSyncFlags：這個值以位元遮罩形式表示，用於控制W32time如何選擇其站台以外的時間來源。可能的值為0、1及2  1. 這個值若設為0(無)，表示時間用戶端不應嘗試與站台外進行時間同步 2. 這個值若設為1(PdcOnly)，表示當用戶端必須與其站台以外的夥伴進行時間同步時，只有在其他網域做為網域主控站(PDC)模擬器操作主機的電腦可做為同步夥伴使用 3. 這個值若設為2(全部)，則表示可以使用任何同步夥伴。如果未設定NT5DS值，就會忽略這個值。預設值是十進位2(十六進位0x02)    * ResolvePeerBackoffMinutes：這個值(以分鐘表示)用於控制W32time在前次嘗試失敗後，於嘗試解析DNS名稱前等候的時間長度。預設值是15分鐘    * ResolvePeerBackoffMaxTimes：這個值用於控制W32time在重新啟動探索處理程序之前，嘗試解析DNS名稱的次數。DNS名稱解析每失敗一次，下次嘗試之前等候的時間長度都將是前次時間長度的兩倍。預設值是7次嘗試    * SpecialPollInterval：這個NTP用戶端值以秒鐘表示，用於控制當手動設定的時間來源設定為使用特殊輪詢間隔時，該時間來源的輪詢頻率。如果NTPServer設定已啟用SpecialInterval旗標，用戶端會使用設定為SpecialPollInterval的值(而不是MinPollInterval和MaxPollInterval值)來判定輪詢時間來源的頻率。預設值是1024秒    * EventLogFlags：這個值是位元遮罩，用於控制可記錄到事件檢視器中系統記錄檔的事件。這個值若設為0x1，表示每次偵測到時間跳躍時，W32time都會建立事件。這個值若設為0x2，表示每次發生時間來源變更時，W32time都會建立事件。因為它是位元遮罩值，所以設定0x3(0x1加上0x2)表示時間跳躍和時間來源變更都會留下紀錄 | 電腦設定\系統管理範本\系統\Windows時間服務\時間提供者\設定Windows NTP用戶端 | 啟用， NTP Server：time.nist.gov 類型： NT5DS CrossSiteSyncFlags：2 ResolvePeerBackoffMinutes：15 ResolvePeerBackoffMaxTimes：7 SpecialPollInterval：3600 EventLogFlags：0 | CCE-ID：CCE-44016-4 |
| 55 | Windows10 Computer Settings | TWGCB-01-005-0055 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉Microsoft Store的存取權 | * 此項原則設定指定是否使用Microsoft Store服務尋找應用程式來開啟具有未處理檔案類型或通訊協定關聯的檔案 * 當使用者所開啟的檔案類型或通訊協定與電腦上任何應用程式都沒有關聯時，使用者可以選擇使用本機應用程式或Microsoft Store服務來尋找應用程式 * 如果啟用此項原則設定，將會移除「開啟檔案」對話方塊中的「在Microsoft Store尋找應用程式」項目 * 如果停用或未設定此項原則設定，使用者將可以使用Microsoft Store服務，而且還可以在「開啟檔案」對話方塊中使用Microsoft Store項目 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Microsoft Store的存取權 | 啟用 | CCE-ID：CCE-43028-0 |
| 56 | Windows10 Computer Settings | TWGCB-01-005-0056 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉透過HTTP下載印表機驅動程式 | * 此項原則設定可以指定是否允許這個用戶端透過HTTP下載印表機驅動程式套件 * 如果要設定HTTP列印，需要透過HTTP下載不在Windows CD上或未與印表機隨附的驅動程式 * 注意：此項原則設定不會禁止用戶端透過HTTP在內部網路或網際網路上的印表機進行列印。它只會禁止下載尚未在本機安裝的驅動程式 * 如果啟用此項原則設定，將無法透過HTTP下載列印驅動程式 * 如果停用或未設定此項原則設定，使用者可以透過HTTP下載列印驅動程式 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉透過HTTP下載印表機驅動程式 | 啟用 | CCE-ID：CCE-42395-4 |
| 57 | Windows10 Computer Settings | TWGCB-01-005-0057 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉事件檢視器"Events.asp"連結 | * 此項原則設定決定是否可以在事件檢視器應用程式中使用"Events.asp"超連結 * 事件檢視器通常會讓所有HTTP(S)URL變成按一下即可啟動網際網路瀏覽器的超連結。另外，如果是由Microsoft元件所建立的事件，「其他資訊」將會置放在描述文字的最後。此文字包含一個連結(URL)，按一下即可傳送該事件相關資訊到Microsoft，並讓使用者進一步瞭解該事件發生的原因 * 若啟用此設定，將不會啟動事件描述URL連結，且在描述文字的最後不會顯示「其他資訊」文字 * 若停用或未設定此設定，使用者可以按一下此超連結，這會提示使用者，然後透過網際網路傳送該事件的相關資訊給Microsoft | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉事件檢視器"Events.asp"連結 | 停用 | CCE-ID：CCE-41718-8 |
| 58 | Windows10 Computer Settings | TWGCB-01-005-0058 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉網頁發布和線上訂購精靈的網際網路下載 | * 此項原則設定決定Windows是否應該為網頁發布精靈和線上訂購精靈下載提供者清單 * 這些精靈可以讓使用者從提供線上儲存和相片列印服務的公司清單中選取。預設狀況下，除了登錄中指定的提供者之外，Windows也會顯示從Windows網站下載的提供者 * 若啟用此設定，Windows將不會下載提供者，而只會顯示本機登錄中快取的服務提供者 * 若停用或未設定此設定，當使用者使用網頁發布精靈或線上訂購精靈時，將會下載提供者清單 * 如需詳細資訊，請參閱網頁發佈精靈和線上訂購精靈文件(包含指定登錄中服務提供者的細節) | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉網頁發布和線上訂購精靈的網際網路下載 | 啟用 | CCE-ID：CCE-42917-5 |
| 59 | Windows10 Computer Settings | TWGCB-01-005-0059 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉HTTP上的列印 | * 此項原則設定決定是否允許使用者透過HTTP列印 * 透過HTTP列印可讓使用者列印到內部網路與網際網路上的印表機 * 注意：此項設定只會影響網際網路列印的用戶端，而不會禁止讓這台電腦成為網際網路列印伺服器，以及作為可以透過HTTP使用的共用印表機 * 若啟用此設定，將禁止使用者透過HTTP列印到網際網路印表機 * 若停用或未設定此設定，使用者將可以選擇透過HTTP列印到網際網路印表機 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉HTTP上的列印 | 啟用 | CCE-ID：CCE-44171-7 |
| 60 | Windows10 Computer Settings | TWGCB-01-005-0060 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉搜尋小幫手內容檔更新 | * 此項原則設定決定搜尋小幫手是否應該在本機與網際網路進行搜尋時，自動下載內容更新 * 當使用者搜尋本機電腦或網際網路時，搜尋小幫手有時會連線到Microsoft下載更新過的隱私權原則和其他用來格式化及顯示結果的內容檔 * 如果啟用此項原則設定，搜尋小幫手將不會在進行搜尋時下載內容更新 * 如果停用或未設定此項原則設定，除非使用者使用的是傳統搜尋，否則搜尋小幫手將會下載內容更新 * 注意：網際網路搜尋還是會將搜尋文字和與搜尋的相關資訊傳送給Microsoft和使用者選用的搜尋提供者。選擇傳統搜尋將會完全關閉搜尋小幫手的功能 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉搜尋小幫手內容檔更新 | 啟用 | CCE-ID：CCE-42313-7 |
| 61 | Windows10 Computer Settings | TWGCB-01-005-0061 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉檔案及資料夾的「發布到網站」工作 | * 此項原則設定決定「Windows」資料夾的檔案和資料夾工作是否有「將此檔案發布到網站」、「將此資料夾發布到網站」或「將選取項目發布到網站」選項 * 網頁發布精靈可以用來下載提供者清單，並讓使用者發布內容到網站 * 若啟用此設定，將會從「Windows」資料夾的檔案和資料夾工作中移除這些工作 * 若停用或未設定此設定，將會顯示這些工作 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉檔案及資料夾的「發布到網站」工作 | 啟用 | CCE-ID：CCE-43826-7 |
| 62 | Windows10 Computer Settings | TWGCB-01-005-0062 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉個人化手寫資料共用 | * 此項原則設定決定是否關閉手寫辨識個人化工具中的資料共用。手寫辨識個人化工具讓 Tablet PC使用者能夠提供書寫範本，根據個人的書寫風格調整手寫辨識方式。這個工具可以選擇性地與Microsoft共用使用者的書寫範本，以改進未來Windows版本中的手寫辨識功能。此工具會產生報告並透過安全連線傳給Microsoft * 如果啟用此項原則，Tablet PC使用者無法選擇將手寫辨識個人化工具中的書寫範本與Microsoft共用 * 如果停用此項原則，手寫辨識個人化工具中Tablet PC使用者書寫範本將與Microsoft共用 * 如果未設定此項原則，則TabletPC使用者可以選擇是否要將他們在手寫辨識個人化工具中的書寫範本與Microsoft共用 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉個人化手寫資料共用 | 啟用 | CCE-ID：CCE-42359-0 |
| 63 | Windows10 Computer Settings | TWGCB-01-005-0063 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉手寫辨識錯誤報告 | * 此項原則設定決定是否關閉手寫辨識錯誤報告工具。使用者可以使用手寫辨識錯誤報告工具來報告在「TabletPC輸入面板」中發生的錯誤。此工具可產生錯誤報告，並透過安全連線將報告傳輸至Microsoft，Microsoft將使用這些錯誤報告來改善未來Windows版本中的手寫辨識功能 * 如果啟用此項原則，使用者將無法啟動手寫辨識錯誤報告工具，或是將錯誤報告傳送給Microsoft * 如果停用或未設定此項原則，則TabletPC使用者可以將手寫辨識錯誤報告給Microsoft | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉手寫辨識錯誤報告 | 啟用 | CCE-ID：CCE-41598-4 |
| 64 | Windows10 Computer Settings | TWGCB-01-005-0064 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉「訂購沖印」圖片工作 | * 此項原則設定指定「Windows」資料夾的圖片工作是否有「線上訂購沖印」工作。「線上訂購沖印」精靈可用來下載提供者清單，並讓使用者線上訂購沖印 * 若啟用此設定，將從「Windows檔案總管」資料夾中移除「線上訂購沖印」圖片工作 * 若停用或未設定此設定，將顯示該工作 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉「訂購沖印」圖片工作 | 啟用 | CCE-ID：CCE-43046-2 |
| 65 | Windows10 Computer Settings | TWGCB-01-005-0065 | 系統\網際網路通訊管理\網際網路通訊設定 | 如果URL連線正在參照Microsoft.com時，關閉註冊 | * 此項原則設定指定Windows註冊精靈是否可以連線到Microsoft.com進行線上註冊 * 如果啟用此項原則設定，將會禁止使用者連線到Microsoft.com進行線上註冊，因此使用者將無法在線上註冊Windows * 如果停用或未設定此項原則設定，則使用者可以連線到Microsoft.com完成線上Windows註冊 * 請注意，註冊是可省略的，而且可能需要送出某些個人資訊給Microsoft。不過，Windows產品啟用則是必要步驟，但不需要送出任何個人資訊(除了居住的國家/地區外) | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\如果URL連線正在參照Microsoft.com時，關閉註冊 | 啟用 | CCE-ID：CCE-43036-3 |
| 66 | Windows10 Computer Settings | TWGCB-01-005-0066 | 系統\網際網路通訊管理\網際網路通訊設定 | 如果URL連線正在參照Microsoft.com時，關閉網際網路連線精靈 | * 此項原則設定指定網際網路連線精靈是否可以連線到Microsoft下載網際網路服務提供者(ISP)清單 * 如果啟用此項原則設定，網際網路連線精靈中的「選擇網際網路服務提供者清單」路徑將導致精靈結束。這會阻止使用者擷取位於Microsoft伺服器上的ISP清單 * 如果停用或未設定此項原則設定，使用者將可以連線到Microsoft下載其區域的ISP清單 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\如果URL連線正在參照Microsoft.com時，關閉網際網路連線精靈 | 啟用 | CCE-ID：CCE-42453-1 |
| 67 | Windows10 Computer Settings | TWGCB-01-005-0067 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉Windows錯誤報告 | * 此項原則設定控制是否向Microsoft報告錯誤 * 錯誤報告是用來報告系統或應用程式失敗或停止回應的相關資訊，並用來改進產品的品質 * 如果啟用此項原則設定，使用者將無法報告錯誤 * 如果停用或未設定此項原則設定，可以透過網際網路或機關的檔案共用向Microsoft報告錯誤。此項原則設定會覆寫任何從控制台對報告錯誤所做的使用者設定 * 此外，也可以參閱「電腦設定/系統管理範本/Windows元件/Windows錯誤報告」中的「設定錯誤報告」、「顯示錯誤通知」和「停用Windows錯誤報告」原則設定 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows錯誤報告 | 啟用 | CCE-ID：CCE-41520-8 |
| 68 | Windows10 Computer Settings | TWGCB-01-005-0068 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉網際網路檔案關聯服務 | * 此項原則設定指定是否使用Microsoft網站服務尋找應用程式來開啟具有未處理檔案關聯的檔案 * 當使用者所開啟檔案之副檔名與電腦上任何應用程式都沒有關聯時，使用者可以選擇使用本機應用程式或網站服務來尋找應用程式 * 如果啟用此項原則設定，則會移除使用網站服務來開啟未處理檔案關聯的連結和對話方塊 * 如果停用或未設定此項原則設定，使用者將可以使用網站服務 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉網際網路檔案關聯服務 | 啟用 | CCE-ID：CCE-43045-4 |
| 69 | Windows10 Computer Settings | TWGCB-01-005-0069 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉Windows Messenger客戶經驗改進計畫 | * 此項原則設定指定Windows Messenger是否收集關於Windows Messenger軟體和服務使用情形的匿名資訊 * 使用者可以透過客戶經驗改進計畫讓Microsoft收集關於產品使用情形的匿名資訊。這項資訊將用來改善未來上市的產品 * 如果啟用此項原則設定，Windows Messenger將不會收集使用資訊，而且也不會顯示啟用收集使用資訊的使用者設定 * 如果停用此項原則設定，Windows Messenger將收集匿名使用資訊，而且不會顯示該設定 * 如果未設定此項原則設定，使用者將能選擇參加，並允許資料收集 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows Messenger客戶經驗改進計畫 | 啟用 | CCE-ID：CCE-43389-6 |
| 70 | Windows10 Computer Settings | TWGCB-01-005-0070 | 進階稽核原則設定 | 稽核驗證認證 | * 此項原則設定可讓使用者稽核因使用者帳戶登入認證的驗證測試而產生的事件 * 只有在授權可以使用那些認證的電腦上，才會發生這個子類別中的事件。如果是網域帳戶，則網域控制站具有授權。如果是本機帳戶，則本機電腦具有授權 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶登入\稽核驗證認證 | 成功與失敗 | CCE-ID：CCE-41615-6 |
| 71 | Windows10 Computer Settings | TWGCB-01-005-0071 | 進階稽核原則設定 | 稽核電腦帳戶管理 | * 此項原則設定可稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 * 如果設定此項原則，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則，則不會在電腦帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核電腦帳戶管理 | 成功 | CCE-ID：CCE-42031-5 |
| 72 | Windows10 Computer Settings | TWGCB-01-005-0072 | 進階稽核原則設定 | 稽核其他帳戶管理事件 | * 此項原則設定可讓使用者稽核因這個類別未涵蓋的其他使用者帳戶變更而產生的事件，例如： * 已存取使用者帳戶的密碼雜湊。這一般是在Active Directory管理工具密碼移轉期間發生 * 已呼叫密碼原則檢查API。在惡意應用程式測試原則以減少密碼字典攻擊期間的嘗試次數時，呼叫這個功能會是一種攻擊 * 下列群組原則路徑下的預設網域群組原則變更： * 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則 * 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則 * 注意：套用原則設定時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核其他帳戶管理事件 | 成功與失敗 | CCE-ID：CCE-42317-8 |
| 73 | Windows10 Computer Settings | TWGCB-01-005-0073 | 進階稽核原則設定 | 稽核安全性群組管理 | * 此項原則設定可稽核因安全性群組變更而產生的事件，例如： * 建立、變更或刪除安全性群組 * 在安全性群組中新增或移除成員 * 變更群組類型 * 如果設定此項原則設定，則會在嘗試變更安全性群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在安全性群組變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核安全性群組管理 | 成功與失敗 | CCE-ID：CCE-43130-4 |
| 74 | Windows10 Computer Settings | TWGCB-01-005-0074 | 進階稽核原則設定 | 稽核使用者帳戶管理 | * 此項原則設定可稽核使用者帳戶的變更。包含下列事件： * 建立、變更、刪除、重新命名、停用、啟用、鎖定或解除鎖定使用者帳戶 * 設定或變更使用者帳戶的密碼 * 將安全性識別碼(SID)新增到使用者帳戶的SID歷程記錄 * 設定目錄服務還原模式密碼 * 變更管理使用者帳戶的權限 * 備份或還原認證管理員認證 * 如果設定此項原則設定，則會在嘗試變更使用者帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在使用者帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核使用者帳戶管理 | 成功與失敗 | CCE-ID：CCE-42410-1 |
| 75 | Windows10 Computer Settings | TWGCB-01-005-0075 | 進階稽核原則設定 | 稽核建立處理程序 | * 此項原則設定可稽核建立或啟動處理程序時產生的事件，也會稽核建立處理程序的應用程式或使用者名稱 * 如果設定此項原則設定，則會在建立處理程序時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在建立處理程序時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核建立處理程序 | 成功 | CCE-ID：CCE-43062-9 |
| 76 | Windows10 Computer Settings | TWGCB-01-005-0076 | 進階稽核原則設定 | 稽核帳戶鎖定 | * 此項原則設定可稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 * 若設定此原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 * 登入事件對於了解使用者活動以及偵測潛在的攻擊是十分重要的 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核帳戶鎖定 | 成功與失敗 | CCE-ID：CCE-42601-5 |
| 77 | Windows10 Computer Settings | TWGCB-01-005-0077 | 進階稽核原則設定 | 稽核登出 | * 此項原則設定可稽核因關閉登入工作階段而產生的事件。這些事件發生於被存取的電腦上。如果是互動式登出，則會在使用者帳戶登入的電腦上產生安全性稽核事件 * 如果設定此項原則設定，則會在關閉登入工作階段時產生稽核事件。成功稽核會記錄成功關閉工作階段嘗試，而失敗稽核則會記錄失敗關閉工作階段嘗試 * 如果未設定此項原則設定，則不會在關閉登入工作階段時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核登出 | 成功 | CCE-ID：CCE-41727-9 |
| 78 | Windows10 Computer Settings | TWGCB-01-005-0078 | 進階稽核原則設定 | 稽核登入 | * 此項原則設定可讓使用者稽核因電腦上的使用者帳戶登入嘗試而產生的事件 * 這個子類別中的事件是與建立登入工作階段有關，而且發生在被存取的電腦上。如果是互動式登入，則會在使用者帳戶登入的電腦上產生安全性稽核事件。如果是網路登入(如存取網路上的共用資料夾)，則會在裝載資源的電腦上產生安全性稽核事件。包含下列事件： * 成功登入嘗試 * 失敗登入嘗試 * 使用明確認證的登入嘗試。處理程序嘗試明確指定該帳戶的認證來登入帳戶時，會產生這個事件。這最常發生於批次登入設定(如排定的工作或使用RUNAS命令時) * 已篩選安全性識別碼(SID)且不允許其登入 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核登入 | 成功與失敗 | CCE-ID：CCE-41786-5 |
| 79 | Windows10 Computer Settings | TWGCB-01-005-0079 | 進階稽核原則設定 | 稽核特殊登入 | * 此項原則設定可稽核因特殊登入而產生的事件，例如： * 使用特殊登入，這是具有管理員同等權限而且可以用來將處理程序提高為較高等級的登入 * 特殊群組成員的登入。特殊群組可讓使用者稽核特定群組成員登入網路時產生的事件 * 可在登錄中設定群組安全性識別碼(SID)清單。如果上述任一SID在登入期間被新增至權杖，而且子類別已啟用，則會記錄事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核特殊登入 | 成功 | CCE-ID：CCE-42066-1 |
| 80 | Windows10 Computer Settings | TWGCB-01-005-0080 | 進階稽核原則設定 | 稽核抽取式存放裝置 | * 此項原則設定可稽核存取抽取式存放裝置上之檔案系統物件的使用者嘗試。安全性稽核事件只會針對所有要求之存取類型的所有物件產生 * 如果設定此原則設定，每當有帳戶存取抽取式存放裝置上的檔案系統物件時，就會產生稽核事件。成功稽核會記錄成功的嘗試，失敗稽核會記錄失敗的嘗試 * 如果未設定此原則設定，當有帳戶存取抽取式存放裝置上的檔案系統物件時，就不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核抽取式存放裝置 | 成功 | CCE-ID：CCE-41572-9 |
| 81 | Windows10 Computer Settings | TWGCB-01-005-0081 | 進階稽核原則設定 | 稽核「稽核原則變更」 | * 此項原則設定可稽核安全性稽核原則設定變更，例如： * 稽核原則物件上的設定權限及稽核設定 * 系統稽核原則的變更 * 安全性事件來源的註冊 * 解除安全性事件來源的註冊 * 每個使用者稽核設定的變更 * CrashOnAuditFail值的變更 * 檔案系統或登錄物件上的系統存取控制清單變更 * 特殊群組清單的變更 * 注意：物件的SACL變更而且已啟用原則變更類別時，會進行系統存取控制清單(SACL)變更稽核。啟用物件存取稽核且設定物件的SACL以稽核DACL/擁有者變更時，會稽核判別存取控制清單(DACL)及擁有權變更 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核「稽核原則變更」 | 成功與失敗 | CCE-ID：CCE-43865-5 |
| 82 | Windows10 Computer Settings | TWGCB-01-005-0082 | 進階稽核原則設定 | 稽核驗證原則變更 | * 此項原則設定可稽核因驗證原則變更而產生的事件，例如： * 建立樹系及網域信任 * 修改樹系及網域信任 * 移除樹系及網域信任 * 變更下列位置下的Kerberos原則：電腦設定\Windows設定\安全性設定\帳戶原則\Kerberos原則 * 將下列任何使用者權限授與使用者或群組： * 從網路存取這台電腦 * 允許本機登入 * 允許透過終端機服務登入 * 以批次工作登入 * 以服務方式登入 * 命名空間衝突。例如，新信任的名稱與現有命名空間名稱相同時 * 如果設定此項原則設定，則會在嘗試變更驗證原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更驗證原則時產生稽核事件 * 注意：套用群組原則時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核驗證原則變更 | 成功 | CCE-ID：CCE-43416-7 |
| 83 | Windows10 Computer Settings | TWGCB-01-005-0083 | 進階稽核原則設定 | 稽核機密特殊權限使用 | * 此項原則設定可稽核使用機密特殊權限(使用者權限)時產生的事件，例如： * 呼叫特許服務 * 呼叫下列其中一種權限：  1. 當成作業系統的一部分 2. 備份檔案及目錄 3. 建立權杖物件 4. 偵錯程式 5. 讓電腦及使用者帳戶受信賴，以進行委派 6. 產生安全性稽核 7. 在驗證後模擬用戶端 8. 載入及解除載入裝置驅動程式 9. 管理稽核及安全性記錄檔 10. 修改韌體環境值 11. 取代處理程序等級權杖 12. 還原檔案及目錄 13. 取得檔案或其他物件的擁有權  * 如果設定此項原則設定，則會在進行機密特殊權限要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 * 如果未設定此項原則設定，則不會進行機密特殊權限要求時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\特殊權限使用\稽核機密特殊權限使用 | 成功與失敗 | CCE-ID：CCE-43224-5 |
| 84 | Windows10 Computer Settings | TWGCB-01-005-0084 | 進階稽核原則設定 | 稽核IPsec驅動程式 | * 此項原則設定可稽核因IPsec篩選器驅動程式而產生的事件，例如： * IPsec服務的啟動及關閉 * 因完整性檢查失敗而丟棄的網路封包 * 因重新執行檢查失敗而丟棄的網路封包 * 因格式為純文字而丟棄的網路封包 * 接收到具有不正確安全性參數索引(SPI)的網路封包。這可能表示網路卡未正確運作，或需要更新驅動程式 * 無法處理IPsec篩選器 * 如果設定此項原則設定，則會在IPsec篩選器驅動程式操作上產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在IPsec篩選器驅動程式操作上產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核IPsec驅動程式 | 成功與失敗 | CCE-ID：CCE-41593-5 |
| 85 | Windows10 Computer Settings | TWGCB-01-005-0085 | 進階稽核原則設定 | 稽核其他系統事件 | * 此項原則設定可稽核下列任一事件： * Windows防火牆服務及驅動程式的啟動及關閉 * Windows防火牆服務的安全性原則處理 * 加密編譯金鑰檔案與移轉操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核其他系統事件 | 失敗 | CCE-ID：CCE-42399-6 |
| 86 | Windows10 Computer Settings | TWGCB-01-005-0086 | 進階稽核原則設定 | 稽核安全性狀態變更 | * 此項原則設定可稽核因電腦安全性狀態變更而產生的事件，例如下列事件： * 電腦的啟動及關閉 * 系統時間的變更 * 從CrashOnAuditFail復原系統，這是在安全性事件記錄檔已滿且設定CrashOnAuditFail登錄項目時於系統重新啟動之後記錄 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核安全性狀態變更 | 成功與失敗 | CCE-ID：CCE-42615-5 |
| 87 | Windows10 Computer Settings | TWGCB-01-005-0087 | 進階稽核原則設定 | 稽核安全性系統延伸 | * 此項原則設定可稽核與安全性系統延伸或服務相關的事件，例如： * 載入安全性系統延伸(如驗證、通知或安全性封裝)，並向本機安全性授權(LSA)進行註冊。它是用來驗證登入嘗試、提交登入要求，以及任何帳戶或密碼變更，Kerberos及NTLM是安全性系統延伸的範例 * 安裝服務，並向服務控制管理員進行註冊。稽核記錄包含服務名稱、二進位、類型、啟動類型及服務帳戶的相關資訊 * 如果設定此項原則設定，則會在嘗試載入安全性系統延伸時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在嘗試載入安全性系統延伸時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核安全性系統延伸 | 成功與失敗 | CCE-ID：CCE-43772-3 |
| 88 | Windows10 Computer Settings | TWGCB-01-005-0088 | 進階稽核原則設定 | 稽核系統完整性 | * 此項原則設定可稽核會破壞安全性子系統完整性的事件，例如： * 因稽核系統發生問題而無法寫入事件記錄檔的事件 * 使用本機程序呼叫(LPC)連接埠的處理程序，而此連接埠在透過與用戶端位址空間之間的回覆、讀取或寫入來嘗試模擬用戶端的過程中無效 * 偵測到危害系統完整性的遠端程序呼叫(RPC) * 偵測到程式碼完整性判斷為無效之可執行檔的雜湊值 * 危害系統完整性的加密編譯操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核系統完整性 | 成功與失敗 | CCE-ID：CCE-41871-5 |
| 89 | Windows10 Computer Settings | TWGCB-01-005-0089 | 安全性選項\帳戶 | 帳戶：Administrator帳戶狀態 | * 此項原則設定決定要啟用或停用本機Administrator帳戶 * 注意：若在停用Administrator帳戶後嘗試重新啟用此帳戶，而現行Administrator密碼不符合密碼要求時，將無法重新啟用此帳戶。在此情況下，必須由Administrators群組的替代成員重設Administrator帳戶的密碼 | 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 | 停用 | CCE-ID：CCE-43470-4 |
| 90 | Windows10 Computer Settings | TWGCB-01-005-0090 | 安全性選項\帳戶 | 帳戶：封鎖Microsoft帳戶 | * 此原則設定可防止透過「設定」應用程式為Microsoft服務和某些背景服務的單一登入(SSO)身分驗證新增Microsoft帳戶，或者使用Microsoft帳戶對其他應用程式或服務進行單一登入 * 如果啟用此設定，將有2個選項： * 若選取「使用者無法新增Microsoft帳戶」選項，代表現有的已連線帳戶仍可以登入此裝置(並出現在登入螢幕上)。不過使用者無法使用「設定」應用程式新增新的連線帳戶(或將本地帳戶連線至Microsoft帳戶) * 若選取「使用者無法新增Microsoft帳戶或以Microsoft帳戶登入」選項，代表使用者無法新增新的連線帳戶(或將本地帳戶連線至Microsoft帳戶)，或是透過設定使用現有的連線帳戶 * 此設定並不影響為應用程式驗證新增Microsoft帳戶。例如，如果此設定啟用，使用者仍然可以提供一個Microsoft帳戶，透過Mail等應用程式進行驗證，但使用者無法使用Microsoft帳戶為其他應用程式或服務進行單一登入驗證(換句話說，使用者將會收到其他應用程式或服務的驗證提示) | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：封鎖Microsoft帳戶 | 啟用，使用者無法新增Microsoft帳戶或以Microsoft帳戶登入 | CCE-ID：CCE-42434-1 |
| 91 | Windows10 Computer Settings | TWGCB-01-005-0091 | 安全性選項\帳戶 | 帳戶：Guest帳戶狀態 | * 此項原則設定決定啟用或停用Guest帳戶 * 注意：如果停用Guest帳戶，而且「網路存取：共用和安全性模式用於本機帳戶」安全性選項是設定為「僅適用於來賓」，則網路登入(例如，由Microsoft網路伺服器(SMB服務)所執行的網路登入)將會失敗 | 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 | 停用 | CCE-ID：CCE-41528-1 |
| 92 | Windows10 Computer Settings | TWGCB-01-005-0092 | 安全性選項\帳戶 | 帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 | * 此項原則設定決定未受密碼保護的本機帳戶，是否可用來從實體電腦主控台以外的位置登入。如果已啟用，那麼未受密碼保護的本機帳戶將只能藉由電腦鍵盤登入 * 注意： * 不是位於實際安全位置的電腦，應一直針對所有本機使用者帳戶強制執行強式密碼原則。否則，每位實際存取電腦的使用者皆可使用沒有密碼的使用者帳戶登入。這對可攜式電腦來說尤其重要 * 如果將此安全性原則套用到Everyone群組，則任何人都不能透過遠端桌面服務登入 * 此項設定對於使用網域帳戶的登入沒有影響 * 應用程式若使用遠端互動式登入，則可以跳過此項設定 * 遠端桌面服務在舊版的Windows作業系統中稱為「終端機服務」 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 | 啟用 | CCE-ID：CCE-41787-3 |
| 93 | Windows10 Computer Settings | TWGCB-01-005-0093 | 安全性選項\帳戶 | 帳戶：重新命名系統管理員帳戶 | 此項原則設定將重新命名已知的Administrator帳戶，透過使用不同的帳戶名稱與Administrator帳戶之安全性識別碼(SID)相關聯，使得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與密碼組合 | 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 | Renamed\_Admin | CCE-ID：CCE-42970-4 |
| 94 | Windows10 Computer Settings | TWGCB-01-005-0094 | 安全性選項\帳戶 | 帳戶：重新命名來賓帳戶名稱 | 此項原則設定將重新命名已知的Guest帳戶，透過使用不同的帳戶名稱與Guest帳戶之安全性識別碼(SID)相關聯，使得未經授權的人員較不容易猜出此使用者名稱與密碼組合 | 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 | Renamed\_Guest | CCE-ID：CCE-43078-5 |
| 95 | Windows10 Computer Settings | TWGCB-01-005-0095 | 安全性選項\稽核 | 稽核：稽核通用系統物件的存取 | * 此項原則設定決定是否稽核通用系統物件的存取 * 如果啟用此原則，會導致系統物件(如Mutex(互斥)、事件、信號及DOS裝置在建立時便含有預設的系統存取控制清單(SACL)。只有具名的物件會被指定SACL，SACL不會指定給沒有名稱的物件 * 如果也啟用「稽核物件存取」稽核原則，則會稽核這些系統物件的存取 * 注意：設定此項原則設定時，在重新啟動Windows之後，所做的變更才會生效 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\稽核：稽核通用系統物件的存取 | 停用 | CCE-ID：CCE-43276-5 |
| 96 | Windows10 Computer Settings | TWGCB-01-005-0096 | 安全性選項\稽核 | 稽核：稽核備份與還原權限的使用 | * 此項原則設定決定在「稽核特殊權限使用」原則生效時，是否稽核備份與還原權限的使用 * 在「稽核特殊權限使用」啟用時同時啟用此設定，將會對備份或還原的每個檔案產生一個稽核事件 * 如果停用此原則，即使啟用「稽核特殊權限使用」，也不會稽核備份或還原權限的使用 * 注意：在備份時啟用此設定可能會造成大量事件，有時每秒會有數百個事件 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\稽核：稽核備份與還原權限的使用 | 停用 | CCE-ID：CCE-42812-8 |
| 97 | Windows10 Computer Settings | TWGCB-01-005-0097 | 安全性選項\稽核 | 稽核：強制執行稽核原則子類別設定(Windows Vista或更新版本)以覆寫稽核原則類別設定 | * Windows Vista及更新版本的Windows允許使用稽核原則子類別，以更精確的方式來管理稽核原則。在類別層級設定稽核原則，將會覆寫新的子類別稽核原則功能。群組原則只允許稽核原則可以在類別層級設定，而且因為新機器會加入網域或者升級至Windows Vista或更新的版本，所以現有的群組原則可以覆寫新機器的子類別設定。為了讓稽核原則不需變更群組原則即可使用子類別來管理，在Windows Vista與更新版本中有新的登錄值SCENoApplyLegacyAuditPolicy，可防止將類別層級稽核原則套用到群組原則及「本機安全性原則」系統管理工具 * 如果在這裡設定的類別層級稽核原則與目前產生的事件不一致，其原因可能是已設定此登錄機碼 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\稽核：強制執行稽核原則子類別設定(Windows Vista或更新版本)以覆寫稽核原則類別設定 | 啟用 | CCE-ID：CCE-42900-1 |
| 98 | Windows10 Computer Settings | TWGCB-01-005-0098 | 安全性選項\稽核 | 稽核：當無法記錄安全性稽核時，系統立即關機 | * 此項安全性設定決定系統在無法記錄安全性事件時，是否要立即關機 * 如果啟用了此項安全性設定，只要無法記錄安全稽核，系統便會停止。基本上，當安全性稽核記錄檔已滿，且安全性記錄檔的保持方法設為「不要覆寫事件」或「依日期覆寫事件」，便無法再記錄事件 * 如果安全性記錄檔已滿且無法覆寫現有項目，但已啟用此安全性選項，則會出現下列停止錯誤：   STOP：C0000244{AuditFailed}嘗試產生安全性稽核時發生失敗   * 若要修復，系統管理員必須登入、備份記錄檔(可省略)、清除記錄檔，再依需要重設此選項。直到此項原則設定重設之前，除了Administrators群組的成員之外，任何使用者都無法登入此系統，即使安全性記錄檔未滿 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\稽核：當無法記錄安全性稽核時，系統立即關機 | 停用 | CCE-ID：CCE-44180-8 |
| 99 | Windows10 Computer Settings | TWGCB-01-005-0099 | 安全性選項\裝置 | 裝置：允許格式化以及退出抽取式媒體 | * 此安全性設定決定允許哪些人格式化和退出抽取式NTFS媒體 * 此功能可指定給： * Administrators * Administrators以及InteractiveUsers | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\裝置：允許格式化以及退出抽取式媒體 | Administrators and Interactive Users | CCE-ID：CCE-43468-8 |
| 100 | Windows10 Computer Settings | TWGCB-01-005-0100 | 安全性選項\裝置 | 裝置：防止使用者安裝印表機驅動程式 | * 裝置：當連線至共用印表機時防止使用者安裝印表機驅動程式 * 要讓電腦列印至共用的印表機，必須在本機電腦上安裝共用印表機的驅動程式。此安全性設定決定誰可以在連線至共用的印表機時安裝印表機驅動程式。如果啟用此設定，只有Administrators可以在連線至共用印表機時安裝印表機驅動程式。如果停用此設定，任何使用者在連線至共用的印表機時，都可以安裝印表機驅動程式 * 注意：此設定不會影響新增本機印表機的能力。此設定不會影響Administrators | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\裝置：防止使用者安裝印表機驅動程式 | 停用 | CCE-ID：CCE-42362-4 |
| 101 | Windows10 Computer Settings | TWGCB-01-005-0101 | 安全性選項\裝置 | 裝置：CD-ROM存取只限於登入本機的使用者 | * 此項原則設定決定本機使用者和遠端使用者是否能同時存取CD-ROM * 如果啟用此原則，便只允許以互動方式登入的使用者存取抽取式CD-ROM媒體。如果啟用此原則但無人以互動方式登入，便能從網路存取該CD-ROM * 預設值：未定義此原則，且CD-ROM存取並未僅限於本機登入的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\裝置：CD-ROM存取只限於登入本機的使用者 | 停用 | CCE-ID：CCE-42798-9 |
| 102 | Windows10 Computer Settings | TWGCB-01-005-0102 | 安全性選項\裝置 | 裝置：軟碟機存取只限於登入本機的使用者 | * 此項原則設定決定本機使用者和遠端使用者是否能同時存取抽取式軟碟機媒體 * 如果啟用此原則，便只允許以互動方式登入的使用者存取抽取式軟碟機媒體。如果啟用此原則但無人以互動方式登入，便能從網路存取該軟碟機 * 預設值：未定義此原則，且軟碟機存取並未僅限於本機登入的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\裝置：軟碟機存取只限於登入本機的使用者 | 停用 | CCE-ID：CCE-42178-4 |
| 103 | Windows10 Computer Settings | TWGCB-01-005-0103 | 安全性選項\網域成員 | 網域成員：安全通道資料加以數位加密或簽章(自動) | * 此項原則設定決定，網域成員啟動的所有安全通道傳輸是否必須經過簽章或加密 * 當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如NTLM通過驗證及LSA SID/名稱查詢的操作 * 此項原則設定決定網域成員啟動的所有安全通道傳輸是否符合最低安全性需求，以及是否必須經過簽章或加密 * 如果啟用此項原則，那麼將不會建立安全通道，除非已交涉所有安全通道傳輸的簽章或加密 * 如果停用此項原則，那麼所有安全通道傳輸的加密和簽章都會與網域控制站進行交涉，在此情況下，簽章和加密的等級是根據網域控制站的版本以及下列兩項原則的設定而定： * 網域成員：安全通道資料加以數位加密(可能的話) * 網域成員：安全通道資料加以數位簽章(自動) * 注意： * 如果啟用此原則，則原則「網域成員：安全通道資料加以數位簽章(可能的話)」假設已被啟用，而不考慮其目前的設定。這將確保網域成員至少嘗試交涉安全通道傳輸的簽章 * 透過安全通道傳輸的登入資訊一定會經過加密，無論「所有」其他安全通道傳輸的加密是否已進行交涉 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位加密或簽章(自動) | 啟用 | CCE-ID：CCE-41762-6 |
| 104 | Windows10 Computer Settings | TWGCB-01-005-0104 | 安全性選項\網域成員 | 網域成員：安全通道資料加以數位加密(可能的話) | * 此項原則設定決定網域成員是否嘗試為其所啟動的所有安全通道傳輸交涉加密 * 當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如NTLM通過驗證LSA SID/名稱查詢之類的操作 * 如果啟用此項原則設定，則網域成員將要求所有安全通道傳輸的加密。如果網域控制站支援所有安全通道傳輸的加密，則所有安全通道傳輸都會經過加密。否則，只有透過安全通道傳輸的登入資訊才會經過加密 * 如果停用此項原則設定，則網域成員不會嘗試交涉安全通道加密 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位加密(可能的話) | 啟用 | CCE-ID：CCE-44137-8 |
| 105 | Windows10 Computer Settings | TWGCB-01-005-0105 | 安全性選項\網域成員 | 網域成員：安全通道資料加以數位簽章(自動) | * 此項原則設定決定網域成員是否嘗試為其所啟動的所有安全通道傳輸交涉簽章。當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如NTLM通過驗證及LSA SID/名稱查詢的操作 * 如果啟用此項原則設定，則網域成員將要求所有安全通道傳輸的簽章。如果網域控制站支援所有安全通道傳輸的簽章，則所有安全通道傳輸都會經過簽章，如此能確保它不會在傳送時遭到竄改 * 注意：如果啟用「網域成員：安全通道資料加以數位加密或簽章(自動)」，則會假設此項原則為啟用狀態，無論目前設定為何 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位簽章(自動) | 啟用 | CCE-ID：CCE-41773-3 |
| 106 | Windows10 Computer Settings | TWGCB-01-005-0106 | 安全性選項\網域成員 | 網域成員：停用電腦帳戶密碼變更 | * 此項原則設定決定是否定期變更網域成員的電腦帳戶密碼 * 如果啟用此設定，網域成員便不會嘗試變更其電腦帳戶密碼 * 如果停用此設定，網域成員將嘗試依「網域成員：最長電腦帳戶密碼有效期」的設定，來變更電腦帳戶密碼，預設為每隔30天 * 注意： * 此項原則設定不應啟用。電腦帳戶密碼是用於建立成員和網域控制站，以及網域內網域控制站之間的安全通道通訊。一旦建立，便會使用安全通道來傳輸建立驗證和授權決策所需的敏感資訊 * 在嘗試支援使用相同電腦帳戶的雙重開機情況下，不應使用此設定。如果要對連結相同網域的兩個安裝執行雙重開機，請指定不同電腦名稱給這兩個安裝 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：停用電腦帳戶密碼變更 | 停用 | CCE-ID：CCE-42856-5 |
| 107 | Windows10 Computer Settings | TWGCB-01-005-0107 | 安全性選項\網域成員 | 網域成員：最長電腦帳戶密碼有效期 | 此項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：最長電腦帳戶密碼有效期 | 30天以下，但須大於0天 | CCE-ID：CCE-41710-5 |
| 108 | Windows10 Computer Settings | TWGCB-01-005-0108 | 安全性選項\網域成員 | 網域成員：要求增強式(Windows 2000或更新)工作階段金鑰 | * 此項原則設定決定加密的安全通道資料是否需要128位元的金鑰長度 * 當電腦加入網域時，會建立電腦帳戶。之後啟動系統時，系統會使用電腦帳戶密碼在該網域內建立一個具有網域控制站的安全通道。此安全通道用來執行諸如NTLM通過驗證或LSA SID/名稱查詢之類的操作 * 如果啟用此項原則設定，除非能執行128位元加密，否則不會建立安全通道 * 如果停用此項原則設定，則會與網域控制站交涉金鑰長度 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：要求增強式(Windows 2000或更新)工作階段金鑰 | 啟用 | CCE-ID：CCE-41474-8 |
| 109 | Windows10 Computer Settings | TWGCB-01-005-0109 | 安全性選項\互動式登入 | 互動式登入：不要顯示上次登入 | * 此項原則設定決定是否要在Windows登入畫面顯示上次登入電腦的使用者名稱 * 如果啟用此原則，登入畫面不會顯示上次順利登入的使用者名稱 * 如果停用此原則，將會顯示上次登入的使用者名稱 | 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 | 啟用 | CCE-ID：CCE-41574-5 |
| 110 | Windows10 Computer Settings | TWGCB-01-005-0110 | 安全性選項\互動式登入 | 互動式登入：不要求按CTRL+ALT+DEL鍵 | * 此項原則設定決定是否需要按CTRL+ALT+DEL後，使用者才能登入 * 如果啟用此原則，使用者不需要按CTRL+ALT+DEL便可登入。不需要按CTRL+ALT+DEL會讓使用者容易受到嘗試攔截使用者密碼的入侵。使用者登入前需要按CTRL+ALT+DEL，這可確保使用者輸入密碼時，以受信任的路徑進行通訊 * 如果停用此原則，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) | 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 | 停用 | CCE-ID：CCE-42781-5 |
| 111 | Windows10 Computer Settings | TWGCB-01-005-0111 | 安全性選項\互動式登入 | 互動式登入：電腦帳戶鎖定閾值 | * 只會在啟用Bitlocker以保護OS磁碟區的電腦上強制執行電腦鎖定原則。請確定已啟用適當的修復密碼備份原則 * 此項原則設定決定了導致電腦鎖定的失敗登入嘗試次數。要修復鎖定的電腦，只能在主控台提供修復金鑰。使用者可以設定介於1到999之間的失敗登入嘗試值。如果將值設定為0，電腦將永遠不會鎖定。1到3的值將被解譯為4 * 在工作站或成員伺服器上，在按下CTRL+ALT+DELETE要登入或要解除鎖定受保護的螢幕保護裝置時若輸入錯誤的密碼，都算是失敗的登入嘗試 | 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：電腦帳戶鎖定閾值 | 5次不正確的登入嘗試 | CCE-ID：CCE-41561-2 |
| 112 | Windows10 Computer Settings | TWGCB-01-005-0112 | 安全性選項\互動式登入 | 互動式登入：電腦未使用時間限制 | Windows會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時執行螢幕保護裝置並鎖定該工作階段 | 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：電腦未使用時間限制 | 900秒以下，但須大於0秒 | CCE-ID：CCE-43844-0 |
| 113 | Windows10 Computer Settings | TWGCB-01-005-0113 | 安全性選項\互動式登入 | 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 | * 所有先前使用者的登入資訊存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用時，則仍然可以登入 * 如果網域控制站無法使用，且未快取使用者的登入資訊時，則會提示使用者下列訊息：「目前無可用的登入伺服器來服務登入請求」 * 在此原則設定中，零值會停用登入快取。若值超過50，則只會快取50次登入嘗試 | 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：網域控制站無法使用時，要快取的先前登入次數 | 2次以下 | CCE-ID：CCE-44148-5 |
| 114 | Windows10 Computer Settings | TWGCB-01-005-0114 | 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 | 此項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先提醒使用者 | 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 | 14天以上 | CCE-ID：CCE-41504-2 |
| 115 | Windows10 Computer Settings | TWGCB-01-005-0115 | 安全性選項\互動式登入 | 互動式登入：要求網域控制站驗證以解除鎖定工作站 | * 必須提供登入資訊才能夠將鎖定的電腦解除鎖定。對於網域帳戶而言，此安全性設定決定是否必須與網域控制站連絡，才能將電腦解除鎖定工作站 * 如果停用此設定，使用者便可以使用快取的認證來將電腦解除鎖定 * 如果啟用此設定，網域控制站便必須驗證用以解除鎖定電腦的網域帳戶 | 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：要求網域控制站驗證以解除鎖定工作站 | 停用 | CCE-ID：CCE-44305-1 |
| 116 | Windows10 Computer Settings | TWGCB-01-005-0116 | 安全性選項\互動式登入 | 互動式登入：智慧卡移除操作 | * 此項原則設定決定當登入使用者的智慧卡從智慧卡讀卡機移除時要執行的動作。選項如下： * 沒有動作 * 鎖定工作站 * 強制登出 * 如果是遠端桌面服務工作階段則中斷連線 * 如果設定為「鎖定工作站」，則會在智慧卡移除時鎖定工作站，讓使用者帶著智慧卡離開，同時繼續保護工作階段 * 如果設定為「強制登出」，則會在智慧卡移除時，自動將使用者登出 * 如果設定為「如果是遠端桌面服務工作階段則中斷連線」，則會在智慧卡移除時中斷工作階段的連線，而不會將使用者登出。這能讓使用者稍後插入智慧卡並繼續工作階段，或是在配備智慧卡讀取裝置的電腦，無須再登入一次。如果工作階段是本機，則此原則的功能與「鎖定工作站」相同 * 預設值：未定義此原則，這表示系統會將它視為「沒有動作」 * 在Windows Vista和更新的版本中，若要讓此設定生效，必須啟動智慧卡移除原則服務 | 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：智慧卡移除操作 | 鎖定工作站 | CCE-ID：CCE-42120-6 |
| 117 | Windows10 Computer Settings | TWGCB-01-005-0117 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(自動) | * 此安全性設定決定SMB用戶端元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理) 的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此原則設定決定允許和SMB伺服器進一步通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此原則，Microsoft網路用戶端將不會和Microsof網路伺服器通訊，除非該伺服器同意執行SMB封包簽章 * 若停用此原則，會在用戶端和伺服器之間交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。在Windows 2000及更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低 | 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：數位簽章用戶端的通訊(自動) | 啟用 | CCE-ID：CCE-41840-0 |
| 118 | Windows10 Computer Settings | TWGCB-01-005-0118 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意) | * 此項原則設定決定SMB用戶端是否嘗試交涉SMB封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章 * 此項原則設定決定SMB用戶端元件連線至SMB伺服器時，是否嘗試交涉SMB封包簽章 * 若啟用此設定，Microsoft網路用戶端將於建立工作階段時要求伺服器執行SMB封包簽章。若已在伺服器上啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。在Windows2000和更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若用戶端與伺服器端SMB簽章兩者已啟用，且用戶端將建立與伺服器之間的SMB 1.0連線，將會嘗試SMB簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低。此設定只適用於SMB 1.0連線 | 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：數位簽章用戶端的通訊(如果伺服器同意) | 啟用 | CCE-ID：CCE-42253-5 |
| 119 | Windows10 Computer Settings | TWGCB-01-005-0119 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：傳送未加密的密碼到其他廠商的SMB伺服器 | * 如果啟用此項原則設定，將允許伺服器訊息區(SMB)重新導向器在驗證期間將純文字密碼傳送給不支援密碼加密的非Microsoft SMB伺服器 * 傳送未經加密的密碼會有安全性風險 | 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 | 停用 | CCE-ID：CCE-41557-0 |
| 120 | Windows10 Computer Settings | TWGCB-01-005-0120 | 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 | * 此項原則設定決定伺服器訊息區(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 * 系統管理員可使用此原則，控制電腦於何時暫停非使用中的SMB工作階段。若用戶端活動繼續，則會自動重新建立工作階段 * 設定為零值表示在合理的時間範圍內儘速中斷工作階段的連線。最大值是99,999，此值會停用此原則 | 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 | 15分鐘以下，但須大於0分鐘 | CCE-ID：CCE-44361-4 |
| 121 | Windows10 Computer Settings | TWGCB-01-005-0121 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(自動) | * 此項原則設定決定SMB伺服器元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定允許和SMB用戶端進行進一步的通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此設定，Microsoft網路伺服器將不會與Microsoft網路用戶端通訊，除非該用戶端同意執行SMB封包簽章 * 若停用此設定，會在用戶端與伺服器之間交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。在Windows 2000與更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 同樣的，若用戶端SMB簽章是必要的，該用戶端將無法與未啟用封包簽章的伺服器建立工作階段。根據預設值，伺服器端SMB簽章只會在網域控制站中啟用 * 若啟用伺服器端SMB簽章，則將與啟用用戶端SMB簽章的用戶端交涉SMB封包簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低 | 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：數位簽章伺服器的通訊(自動) | 啟用 | CCE-ID：CCE-42884-7 |
| 122 | Windows10 Computer Settings | TWGCB-01-005-0122 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意) | * 此項原則設定決定SMB伺服器是否將和要求SMB封包簽章的用戶端交涉 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定SMB伺服器是否將在SMB用戶端要求SMB封包簽章時進行交涉 * 若啟用此設定，Microsoft網路伺服器將在用戶端要求SMB封包簽章時進行交涉。也就是說，若已在用戶端啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。在Windows 2000與更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若用戶端與伺服器端SMB簽署兩者已啟用，且用戶端建立與伺服器之間的SMB 1.0連線，將會嘗試SMB簽署 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低。此設定只適用於SMB 1.0連線 | 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：數位簽章伺服器的通訊(如果用戶端同意) | 啟用 | CCE-ID：CCE-44027-1 |
| 123 | Windows10 Computer Settings | TWGCB-01-005-0123 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：當登入時數到期時，中斷用戶端連線 | * 此項原則設定決定是否要在超出使用者帳戶的有效登入時數時，將連線到本機電腦的使用者中斷連線。此設定會影響到伺服器訊息區(SMB)元件 * 啟用此原則設定時，便會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 * 如果停用此原則設定，便允許在用戶端的登入時數到期之後，繼續維持建立的用戶端工作階段 | 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 | 啟用 | CCE-ID：CCE-43184-1 |
| 124 | Windows10 Computer Settings | TWGCB-01-005-0124 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：伺服器SPN目標名稱驗證層級 | * 此項原則設定控制具有共用資料夾的電腦或印表機伺服器在服務主體名稱(SPN)上執行的驗證層級，選項如下： * 關閉：SMB伺服器不需要或不會驗證SMB用戶端的SPN * 如果是用戶端所提供則接受：SMB伺服器將會接受與驗證SMB用戶端提供的SPN，並允許當該SPN符合SMB伺服器本身的SPN清單時，建立工作階段。如果SPN不相符，將會拒絕該SMB用戶端的工作階段要求 * 用戶端的要求：SMB用戶端「必須」在工作階段設定中傳送SPN名稱，而且提供的SPN名稱「必須」符合被要求建立連線的SMB伺服器。如果用戶端未提供任何SPN，或是提供的SPN不相符，則會拒絕該工作階段 * SPN是用戶端電腦在使用伺服器訊息區(SMB)通訊協定來建立工作階段時所提供 * 伺服器訊息區(SMB)通訊協定是檔案及列印共用和其他網路作業(例如遠端Windows系統管理)的基礎 * SMB通訊協定支援驗證SMB用戶端提供的驗證二進位大型物件中的SMB伺服器服務主體名稱(SPN)，以防止針對SMB伺服器的類別攻擊(稱為SMB轉送攻擊)。此設定將同時影響SMB1與SMB2 * 所有的Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。此項設定會影響伺服器SMB行為，應該小心評估與測試，以防止檔案與列印服務功能的中斷 | 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：伺服器SPN目標名稱驗證層級 | 如果是用戶端所提供則接受 | CCE-ID：CCE-41486-2 |
| 125 | Windows10 Computer Settings | TWGCB-01-005-0125 | MSS(Legacy) | MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | * 此項原則設定決定電腦是否採取自動登入方式 * 如果設定為啟用，當電腦啟動時，將使用以純文字形式儲存於Registry內之網域、帳號及密碼資訊自動登入該電腦，因此能實體存取電腦的任何人也都能存取該電腦中的一切資訊，包括任何網路或電腦所能連線到的網路在內 * 如果設定為停用，電腦將不採取自動登入方式 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | 停用 | CCE-ID：CCE-42219-6 |
| 126 | Windows10 Computer Settings | TWGCB-01-005-0126 | MSS(Legacy) | MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | * IP source routing可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection, source routed packets are allowed，代表作業系統接受與轉送來源路由封包 * 設為Medium, source routed packets ignored when IP forwarding is enabled，代表作業系統接受但不轉送來源路由封包 * 設為Highest protection, source routing is completely disabled，代表作業系統完全拒絕來源路由封包 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | 啟用，Highest protection, source routing is completely disabled | CCE-ID：CCE-41874-9 |
| 127 | Windows10 Computer Settings | TWGCB-01-005-0127 | MSS(Legacy) | MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | * IP source routing是一種允許傳送者決定資料包通過網路時應該採用IP路由的機制，可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection, source routed packets are allowed，代表作業系統接受與轉送來源路由封包 * 設為Medium, source routed packets ignored when IP forwarding is enabled，代表作業系統接受但不轉送來源路由封包 * 設為Highest protection, source routing is completely disabled，代表作業系統完全拒絕來源路由封包 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | 啟用，Highest protection, source routing is completely disabled | CCE-ID：CCE-41998-6 |
| 128 | Windows10 Computer Settings | TWGCB-01-005-0128 | MSS(Legacy) | MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | * 此項原則設定決定是否允許ICMP重新導向覆寫OSPF產生的路由，意謂著作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，是否要改變其路由表 * 如果設定為啟用，作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，將會改變其路由表 * 如果設定為停用，作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，不會改變其路由表 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 停用 | CCE-ID：CCE-41794-9 |
| 129 | Windows10 Computer Settings | TWGCB-01-005-0129 | MSS(Legacy) | MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | * 此項原則設定決定是否從網路瀏覽列表中移除本台電腦名稱 * 如果設定為啟用，將從網路瀏覽列表中移除本台電腦名稱 * 如果設定為停用，網路瀏覽列表依然保留本台電腦名稱。知道本台電腦名稱之攻擊者，將可能透過網路蒐集本台電腦資訊 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | 啟用 | CCE-ID：CCE-42695-7 |
| 130 | Windows10 Computer Settings | TWGCB-01-005-0130 | MSS(Legacy) | MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | * 此項原則設定決定持續作用的封包多少毫秒會傳送一次，讓TCP藉由傳送持續作用封包，來嘗試驗證閒置連線狀態是否仍然不變 * 如果遠端系統仍然可以連接與運作，就會確認持續作用傳輸在預設的情況下，並不會傳送持續作用封包 * 此項功能可由應用程式在連線時啟用 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | 啟用，300000或5分鐘 | CCE-ID：CCE-41614-9 |
| 131 | Windows10 Computer Settings | TWGCB-01-005-0131 | MSS(Legacy) | MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | * 此項原則設定決定是否啟用IPSec篩選器的預設豁免項目，選項如下： * Allow all exemptions (least secure)：代表「多點傳送廣播，RSVP、Kerberos及ISAKMP流量不受限於IPSec篩選功能」 * Multicast, broadcast, & ISAKMP exempt (best for Windows XP)：代表「Kerberos及RSVP流量並不受IPSec篩選，但多點傳播、廣播及ISAKMP流量都是豁免」 * RSVP, Kerberos, and ISAKMP are exempt：代表「多點傳播和廣播流量並不受IPSec篩選，但RSVP、Kerberos及ISAKMP流量被豁免」 * Only ISAKMP is exempt (recommended for Windows Server 2003)：代表「只有ISAKMP流量是免除IPSec篩選功能」 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | 啟用，Multicast，broadcast，and ISAKMP are exempt(best for Windows XP) | CCE-ID：CCE-42220-4 |
| 132 | Windows10 Computer Settings | TWGCB-01-005-0132 | MSS(Legacy) | MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | * NetBIOS(網路基本輸入/輸出系統)over TCP/IP是一種網路通訊協定，提供簡易的解析方法，可以將登錄在Windows系統上的NetBIOS名稱解析為這些系統所設定的IP位址 * 此項原則設定決定當電腦收到名稱釋放要求時是否釋放它的NetBIOS名稱 * 如果設定為啟用，當電腦收到名稱釋放要求時，不會釋放它的NetBIOS名稱 * 如果設定為停用，當電腦收到名稱釋放要求時，將會釋放它的NetBIOS名稱。惡意的使用者可以利用此通訊協定不需驗證的特質，將名稱衝突的資料包傳送到目標電腦，造成名稱釋放的情形而停止回應查詢，造成目標電腦發生連線斷斷續續的問題，或甚至造成無法使用「網路上的芳鄰」、網域登入、netsend命令，或是無法進行後續的NetBIOS名稱解析 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | 啟用 | CCE-ID：CCE-42327-7 |
| 133 | Windows10 Computer Settings | TWGCB-01-005-0133 | MSS(Legacy) | MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 此項原則設定決定是否允許Internet Router Discovery Protocol(IRDP)自動偵測與設定預設Gateway位址 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 停用 | CCE-ID：CCE-42024-0 |
| 134 | Windows10 Computer Settings | TWGCB-01-005-0134 | MSS(Legacy) | MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | * 此項原則設定決定應用程式搜尋DLL檔的順序 * 如果設定為啟用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 目前目錄 * 在PATH環境變數中列出來的目錄 * 如果設定為停用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 目前目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 在PATH環境變數中列出來的目錄 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | 啟用 | CCE-ID：CCE-42221-2 |
| 135 | Windows10 Computer Settings | TWGCB-01-005-0135 | MSS(Legacy) | MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | * 若啟用螢幕保護裝置的鎖定功能，在螢幕保護裝置啟動到主控台實際自動鎖定之間，Windows設置有一段寬限期。此項原則設定決定寬限期時間(以秒計算) * 可以設定為介於0到255之間的任何數值 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 啟用，5以下，但須大於0 | CCE-ID：CCE-42075-2 |
| 136 | Windows10 Computer Settings | TWGCB-01-005-0136 | MSS(Legacy) | MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 啟用，3以下，但須大於0 | CCE-ID：CCE-42788-0 |
| 137 | Windows10 Computer Settings | TWGCB-01-005-0137 | MSS(Legacy) | MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 啟用，3以下，但須大於0 | CCE-ID：CCE-41750-1 |
| 138 | Windows10 Computer Settings | TWGCB-01-005-0138 | MSS(Legacy) | MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | * 當安全性事件記錄檔大小到達最大可用的百分比時，產生警告 * 預設值沒有指定，當定義此原則時，可以選擇50%、60%、70%、80%或90%等臨界值 * 如果安全性事件記錄檔設定為覆寫，則不會產生警告 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | 啟用，90 | CCE-ID：CCE-41795-6 |
| 139 | Windows10 Computer Settings | TWGCB-01-005-0139 | MSS(Legacy) | MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 此項原則決定當使用撥接網路或VPN連接撥接網路時，可以選擇「儲存密碼」以便快取撥接網路密碼，不需要再連續嘗試撥接時輸入 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 啟用 | CCE-ID：CCE-42023-2 |
| 140 | Windows10 Computer Settings | TWGCB-01-005-0140 | 安全性選項\網路存取 | 網路存取：允許匿名SID/名稱轉譯 | * 此項原則設定決定匿名使用者是否可以請求其他使用者的安全性識別碼(SID)屬性 * 如果啟用此原則，匿名使用者可以請求其他使用者的SID屬性。知道系統管理員SID的匿名使用者可以聯絡已啟用此原則的電腦，且能使用該SID來取得系統管理員的名稱 * 此設定會同時影響「SID轉譯為名稱」與「名稱轉譯為SID」 * 如果停用此原則設定，匿名使用者將無法請求其他使用者的SID屬性 | 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 | 停用 | CCE-ID：CCE-41861-6 |
| 141 | Windows10 Computer Settings | TWGCB-01-005-0141 | 安全性選項\網路存取 | 網路存取：不允許SAM帳戶和共用的匿名列舉 | * 此項原則設定決定是否允許SAM帳戶和共用的匿名列舉 * Windows允許匿名使用者執行特定活動，例如列舉網域帳戶和網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權，而該網域不會保持交互信任時，此功能相當方便。如果想禁止SAM帳戶和共用的匿名列舉，請啟用此原則 | 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 | 啟用 | CCE-ID：CCE-43628-7 |
| 142 | Windows10 Computer Settings | TWGCB-01-005-0142 | 安全性選項\網路存取 | 網路存取：不允許SAM帳戶的匿名列舉 | * 此項原則設定決定授與電腦匿名連線哪些其他權限 * Windows允許匿名使用者執行特定活動，例如列舉網域帳戶和網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權，而該網域不會保持交互信任時，此功能相當方便。如果想禁止SAM帳戶和共用的匿名列舉，請啟用此原則 * 此安全性選項允許在匿名連線中設定其他限制，如下： * 啟用：不允許列舉SAM帳戶。此選項會將資源之安全性權限中的Everyone取代為Authenticated Users * 停用：沒有其他限制。視預設權限而定 | 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 | 啟用 | CCE-ID：CCE-43517-2 |
| 143 | Windows10 Computer Settings | TWGCB-01-005-0143 | 安全性選項\網路存取 | 網路存取：不允許存放網路驗證的密碼與認證 | * 此項原則設定決定認證管理員取得網域驗證時，是否儲存密碼與認證，以供稍後使用 * 如果啟用此設定，認證管理員不會在電腦上儲存密碼與認證 * 如果停用或未設定此原則設定，認證管理員將會在此電腦上存放密碼與認證，以供稍後用於網域驗證 * 注意：設定此項原則設定時，必須重新啟動Windows，變更才會生效 | 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 | 啟用 | CCE-ID：CCE-42974-6 |
| 144 | Windows10 Computer Settings | TWGCB-01-005-0144 | 安全性選項\網路存取 | 網路存取：讓Everyone權限套用到匿名使用者 | * 此項原則設定決定將授與電腦匿名連線哪些其他權限 * Windows允許匿名使用者執行特定活動，例如列舉網域帳戶與網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權限，而該網域不會保持交互信任時，此功能相當方便 * 根據預設值，會從為匿名連線建立的權杖中移除Everyone安全性識別碼(SID)。因此，授與Everyone群組的權限不會套用至匿名使用者。若設定此選項，匿名使用者只能存取已明確取得權限的資源 * 若啟用此原則，Everyone SID會新增至為匿名連線建立的權杖。在此情況下，匿名使用者可存取Everyone群組已取得權限的任何資源 | 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：讓Everyone權限套用到匿名使用者 | 停用 | CCE-ID：CCE-41948-1 |
| 145 | Windows10 Computer Settings | TWGCB-01-005-0145 | 安全性選項\網路存取 | 網路存取：可以匿名存取的具名管道 | 此項原則設定決定哪個通訊工作階段(管道)將擁有允許匿名存取的屬性和權限 | 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：可以匿名存取的具名管道 | 無 | CCE-ID：CCE-43557-8 |
| 146 | Windows10 Computer Settings | TWGCB-01-005-0146 | 安全性選項\網路存取 | 網路存取：可遠端存取的登錄路徑及子路徑 | * 此原則設定決定哪些登錄路徑及子路徑可經由網路存取(不管winreg登錄機碼中存取控制清單(ACL)所列的使用者或群組為何) * 警告：不正確地編輯登錄將會對系統造成嚴重的損害。在變更登錄前，使用者應先備份電腦上任何有價值的資料 | 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：可遠端存取的登錄路徑及子路徑 | * Software\Microsoft\Windows NT\CurrentVersion\Print * Software\Microsoft\Windows NT\CurrentVersion\Windows * System\CurrentControlSet\Control\Print\Printers * System\CurrentControlSet\Services\Eventlog * Software\Microsoft\OLAP Server * System\CurrentControlSet\Control\ContentIndex * System\CurrentControlSet\Control\Terminal Server * System\CurrentControlSet\Control\Terminal Server\UserConfig * System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration * Software\Microsoft\Windows NT\CurrentVersion\Perflib * System\CurrentControlSet\Services\SysmonLog | CCE-ID：CCE-42160-2 |
| 147 | Windows10 Computer Settings | TWGCB-01-005-0147 | 安全性選項\網路存取 | 網路存取：可遠端存取的登錄路徑 | * 此項原則設定決定哪些登錄機碼可經由網路存取(不管winreg登錄機碼中存取控制清單(ACL)所列的使用者或群組為何) * 注意：不正確地編輯登錄將會對系統造成嚴重的損害。在變更登錄前，應先備份電腦上任何有價值的資料 | 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：可遠端存取的登錄路徑 | * System\CurrentControlSet\Control\ProductOptions * System\CurrentControlSet\Control\Server Applications * Software\Microsoft\Windows NT\CurrentVersion | CCE-ID：CCE-42010-9 |
| 148 | Windows10 Computer Settings | TWGCB-01-005-0148 | 安全性選項\網路存取 | 網路存取：限制匿名存取具名管道和共用 | * 此項原則設定決定是否限制匿名存取具名管道和共用 * 啟用時，此項原則設定會將共用和管道的匿名存取限制為以下設定： * 網路存取：可以匿名存取的具名管道 * 網路存取：可以匿名存取的共用 | 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：限制匿名存取具名管道和共用 | 啟用 | CCE-ID：CCE-43105-6 |
| 149 | Windows10 Computer Settings | TWGCB-01-005-0149 | 安全性選項\網路存取 | 網路存取：可以匿名存取的共用 | 此項原則設定決定匿名使用者能夠存取哪個網路共用 | 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：可以匿名存取的共用 | 無 | CCE-ID：CCE-43953-9 |
| 150 | Windows10 Computer Settings | TWGCB-01-005-0150 | 安全性選項\網路存取 | 網路存取：共用和安全性模式用於本機帳戶 | * 此項原則設定決定如何驗證使用本機帳戶的網路登入 * 若此設定設為「傳統，本機使用者以自身身分驗證」，則使用本機帳戶認證的網路登入會使用那些認證進行驗證。「傳統，本機使用者以自身身分驗證」模式可有效控制對資源的存取。使用「傳統」模式，可針對相同資源授與不同類型的存取權限給不同的使用者 * 若此設定設為「僅適用於來賓，本機使用者以Guest驗證」，則使用本機帳戶的網路登入會自動對應到來賓帳戶。使用「僅適用於來賓，本機使用者以Guest驗證」模式，可以等同方式對待所有使用者。所有使用者均驗證為「來賓」，且收到的特定資源存取權限等級相同，即可能是「唯讀」或「修改」 * 注意： * 使用「僅適用於來賓，本機使用者以Guest驗證」模式，可經由網路存取電腦的所有使用者(包括匿名網際網路使用者)都能存取共用資源。必須使用Windows防火牆或其他類似裝置來保護電腦免於未經授權存取的侵害 * 使用「傳統，本機使用者以自身身分驗證」模式，必須使用密碼保護本機帳戶，否則任何人都可使用那些使用者帳戶存取共用系統資源 | 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：共用和安全性模式用於本機帳戶 | 傳統，本機使用者以自身身分驗證 | CCE-ID：CCE-42264-2 |
| 151 | Windows10 Computer Settings | TWGCB-01-005-0151 | 安全性選項\網路安全性 | 網路安全性：允許Local System對NTLM使用電腦身分識別 | * 此項原則設定允許使用交涉的Local System服務在還原使用NTLM驗證時，使用電腦身分識別 * 如果啟用此項原則設定，以Local System執行且使用交涉的服務會使用電腦身分識別。這可能會造成Windows作業系統之間的某些驗證要求失敗並記錄錯誤 * 如果停用此項原則設定，則以Local System執行且使用交涉的服務在還原為NTLM驗證時將會匿名驗證 | 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：允許Local System對NTLM使用電腦身分識別 | 啟用 | CCE-ID：CCE-41597-6 |
| 152 | Windows10 Computer Settings | TWGCB-01-005-0152 | 安全性選項\網路安全性 | 網路安全性：允許LocalSystem NULL工作階段回復 | 使用Local System時，允許NTLM回復NULL工作階段 | 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：允許LocalSystem NULL工作階段回復 | 停用 | CCE-ID：CCE-43898-6 |
| 153 | Windows10 Computer Settings | TWGCB-01-005-0153 | 安全性選項\網路安全性 | 網路安全性：允許對此電腦的PKU2U驗證要求使用線上身分識別 | * 在已加入網域的電腦上預設會關閉此原則。這樣便不會允許使用線上身分識別來向已加入網域的電腦驗證 * 在Windows 10 1607版前，此原則在已加入網域的電腦上預設為停用，在1607版後，此原則預設為啟用 | 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：允許對此電腦的PKU2U驗證要求使用線上身分識別 | 停用 | CCE-ID：CCE-43189-0 |
| 154 | Windows10 Computer Settings | TWGCB-01-005-0154 | 安全性選項\網路安全性 | 網路安全性：設定Kerberos允許的加密類型 | * 此項原則將設定允許Kerberos使用的加密類型 * 如果未選取，則不允許加密類型。此項設定可能會影響與用戶端電腦或服務及應用程式的相容性 * 此項原則設定允許多個選取項目 | 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 | * AES128\_HMAC\_SHA1 * AES256\_HMAC\_SHA1 * 未來的加密類型 | CCE-ID：CCE-41647-9 |
| 155 | Windows10 Computer Settings | TWGCB-01-005-0155 | 安全性選項\網路安全性 | 網路安全性：下次密碼變更時不儲存LAN Manager雜湊數值 | * 此項原則設定決定在下次密碼變更時，是否要儲存新密碼的LAN Manager雜湊值。與加密編譯較強的Windows NT雜湊相比，LM雜湊相對較不安全，並且容易遭到攻擊。因為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 * 注意：Windows 2000 Service Pack 2(SP2)及更新版本提供與舊版Windows (如Microsoft Windows NT 4.0)驗證的相容性 | 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 | 啟用 | CCE-ID：CCE-43657-6 |
| 156 | Windows10 Computer Settings | TWGCB-01-005-0156 | 安全性選項\網路安全性 | 網路安全性：強制限制登入時數 | * 此項原則設定決定使用者連線至本機電腦若超過其使用者帳戶有效的登入時數時，是否要中斷連線，此設定會影響伺服器訊息區(SMB)元件 * 啟用此原則時，若用戶端登入時數到期，會強制中斷用戶端工作階段與SMB伺服器的連線 * 若停用此原則，當用戶端登錄時數到期之後，可以允許保留已建立的用戶端工作階段 | 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：強制限制登入時數 | 啟用 | CCE-ID：CCE-42170-1 |
| 157 | Windows10 Computer Settings | TWGCB-01-005-0157 | 安全性選項\網路安全性 | 網路安全性：LAN Manager驗證等級 | * 此項原則設定決定使用哪種Challenge/Response驗證通訊協定登入網路。此設定將影響用戶端使用的驗證通訊協定層級、交涉的工作階段安全性層級，以及伺服器接受的驗證等級，選項如下： * 傳送LM和NTLM回應：用戶端使用LM和NTLM驗證，絕不使用NTLMv2工作階段安全性；網域控制站接受LM、NTLM及NTLMv2驗證 * 傳送LM和NTLM-如有交涉，使用NTLMv2工作階段安全性：用戶端使用LM和NTLM驗證，而且若伺服器支援，則會使用NTLMv2工作階段安全性；網域控制站接受LM、NTLM及NTLMv2驗證 * 只傳送NTLM回應：用戶端只使用NTLM驗證，而且若伺服器支援，則會使用NTLMv2工作階段安全性；網域控制站接受LM、NTLM及NTLMv2驗證 * 只傳送NTLMv2回應：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；網域控制站接受LM、NTLM及NTLMv2驗證 * 只傳送NTLMv2回應\拒絕LM：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；網域控制站拒絕LM(只接受NTLM與NTLMv2驗證) * 只傳送NTLMv2回應\拒絕LM和NTLM：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；網域控制站拒絕LM和NTLM(只接受NTLMv2驗證) | 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 | 只傳送NTLMv2回應。拒絕LM和NTLM | CCE-ID：CCE-43546-1 |
| 158 | Windows10 Computer Settings | TWGCB-01-005-0158 | 安全性選項\網路安全性 | 網路安全性：LDAP用戶端簽章要求 | * 此項原則設定決定代表發出LDAP BIND要求之用戶端所要求的資料簽章層級，選項如下： * 無：LDAP BIND要求隨呼叫者指定的選項發出 * 交涉簽章：若未啟動傳輸層安全性/安全通訊端層(TLS\SSL)，會隨呼叫者指定的選項以外的LDAP資料簽章選項初始化LDAP BIND要求。若已啟動TLS\SSL，會隨呼叫者指定的選項初始化LDAP BIND要求 * 要求簽章：這與交涉簽章相同。不過，若LDAP伺服器的中繼saslBindInProgress回應未指LDAP流量簽章為必要的，則會告知呼叫者LDAP BIND命令要求失敗 | 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：LDAP用戶端簽章要求 | 交涉簽章 | CCE-ID：CCE-43458-9 |
| 159 | Windows10 Computer Settings | TWGCB-01-005-0159 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 此項原則設定允許用戶端要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，可勾選的安全性設定值選項如下(可複選)： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 | CCE-ID：CCE-42134-7 |
| 160 | Windows10 Computer Settings | TWGCB-01-005-0160 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 此項原則設定允許伺服器要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，可勾選的安全性設定值選項如下(可複選)： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 | CCE-ID：CCE-42842-5 |
| 161 | Windows10 Computer Settings | TWGCB-01-005-0161 | 安全性選項\修復主控台 | 修復主控台：允許自動系統管理登入 | * 此項原則設定決定是否必須在授與系統存取權之前提供Administrator帳戶的密碼 * 如果啟用此原則設定，修復主控台不需要提供密碼，且將會自動登入系統 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\修復主控台：允許自動系統管理登入 | 停用 | CCE-ID：CCE-41475-5 |
| 162 | Windows10 Computer Settings | TWGCB-01-005-0162 | 安全性選項\修復主控台 | 修復主控台：允許軟碟複製以及存取所有磁碟和所有資料夾 | * 啟用此項原則設定將可以使用修復主控台SET命令，此命令可設定下列修復主控台環境變數： * Allow Wild Cards：對某些命令啟用萬用字元支援(例如DEL命令) * Allow All Paths：允許存取電腦上的所有檔案和資料夾 * Allow Removable Media：允許將檔案複製到抽取式媒體，例如磁片 * No Copy Prompt：不要提示正在覆寫現有的檔案 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\修復主控台：允許軟碟複製以及存取所有磁碟和所有資料夾 | 停用 | CCE-ID：CCE-41562-0 |
| 163 | Windows10 Computer Settings | TWGCB-01-005-0163 | 安全性選項\關機 | 關機：允許不登入就將系統關機 | * 此項原則設定決定是否無需登入Windows便能夠將電腦關機 * 啟用此原則時，Windows登入畫面上可以使用「關機」命令 * 停用此原則時，Windows登入畫面上不會顯示將電腦關機的選項。在這種情況下，使用者必須要能順利登入電腦，取得關閉系統使用者權限之後，才能執行系統關機操作 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\關機：允許不登入就將系統關機 | 啟用 | CCE-ID：CCE-43340-9 |
| 164 | Windows10 Computer Settings | TWGCB-01-005-0164 | 安全性選項\關機 | 關機：清除虛擬記憶體分頁檔 | * 此原則設定決定系統關機時是否清除虛擬記憶體分頁檔 * 虛擬記憶體支援使用系統分頁檔交換不使用的記憶體分頁至磁碟。在執行的系統上，此分頁檔由作業系統獨佔開啟，並且受到保護。不過，未設定允許以其他作業系統開機的系統，可能必須確定系統分頁檔在此系統關機時已刪除完畢。這樣可確保可能進入分頁檔的處理程序記憶體中的敏感資料，不會被直接存取分頁檔的未經授權使用者使用 * 當啟用此原則時，在正常關機時會清除系統分頁檔。若啟用此原則設定，當停用休眠時，也會清除休眠檔案(hiberfil.sys) | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\關機：清除虛擬記憶體分頁檔 | 停用 | CCE-ID：CCE-44311-9 |
| 165 | Windows10 Computer Settings | TWGCB-01-005-0165 | 安全性選項\系統加密編譯 | 系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | * 對於Schannel Security Service Provider(SSP)，此項原則設定會停用強度較低的安全通訊端層(SSL)通訊協定，而且只支援傳輸層安全性(TLS)通訊協定作為用戶端以及伺服器(如果適用)連線機制 * 如果啟用此設定，傳輸層安全性/安全通訊端層(TLS/SSL)安全性提供者只會使用FIPS140核准的密碼編譯演算法：3DES與AES用於加密、RSA或ECC公開金鑰密碼編譯用於TLS金鑰交換與驗證，而且只有安全雜湊演算法(SHA1、SHA256、SHA384以及SHA512)用於TLS雜湊需求 * 對於加密檔案系統服務(EFS)，僅支援使用三重資料加密標準(DES)與進階加密標準(AES)加密演算法來加密NTFS檔案系統支援的檔案資料 * 對於遠端桌面服務，它只支援使用三重DES加密演算法來加密遠端桌面服務網路通訊 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | 啟用 | CCE-ID：CCE-42459-8 |
| 166 | Windows10 Computer Settings | TWGCB-01-005-0166 | 安全性選項\系統物件 | 系統物件：要求不區分大小寫用於非Windows子系統 | * 此項原則設定決定是否要強制所有子系統區分大小寫。Win32子系統不會區分大小寫。但是如POSIX等其他子系統的核心支援區分大小寫 * 如果啟用此設定，便會強制所有目錄物件、符號連結及IO物件(包括檔案物件在內)不區分大小寫 * 如果停用此設定，將允許非Windows子系統區分大小寫 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統物件：要求不區分大小寫用於非Windows子系統 | 啟用 | CCE-ID：CCE-41855-8 |
| 167 | Windows10 Computer Settings | TWGCB-01-005-0167 | 安全性選項\系統物件 | 系統物件：加強內部系統物件的預設權限(例如：符號連結) | * 此原則設定決定物件的預設判別存取控制清單(DACL)的強度 * Active Directory維護共用系統資源(例如DOS裝置名稱、Mutex及信號)的全域清單。如此，便可在程序之間找到和共用物件。每種類型的物件都會建立一個預設的DACL，它指定誰可以存取物件和所授與的權限為何 * 若啟用此原則，預設的DACL較強，允許非系統管理員的使用者讀取共用物件，但不允許這些使用者修改不是他們建立的共用物件 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統物件：加強內部系統物件的預設權限(例如：符號連結) | 啟用 | CCE-ID：CCE-44287-1 |
| 168 | Windows10 Computer Settings | TWGCB-01-005-0168 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：內建的Administrator帳戶的管理員核准模式 | * 此項原則設定會控制內建的Administrator帳戶的管理員核准模式行為，選項如下： * 啟用：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 * 停用：內建的Administrator帳戶將以完整的系統管理權限執行所有應用程式 | 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：內建的Administrator帳戶的管理員核准模式 | 啟用 | CCE-ID：CCE-43453-0 |
| 169 | Windows10 Computer Settings | TWGCB-01-005-0169 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：允許UIAccess應用程式不使用安全桌面來提示提升權限 | * 此項原則設定控制使用者介面協助工具(UIAccess或UIA)程式在標準使用者使用提升權限提示時，是否自動停用安全桌面 * 如果設定為啟用，UIA程式，包括Windows遠端協助在內的UIA程式，可自動停用提升權限提示的安全桌面。如果未停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定，提示會出現在互動式使用者的桌面上，而非安全桌面 * 如果設定為停用，只有互動式桌面的使用者才能停用安全桌面，或是停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定才能停用安全桌面 | 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：允許UIAccess應用程式不使用安全桌面來提示提升權限 | 停用 | CCE-ID：CCE-44049-5 |
| 170 | Windows10 Computer Settings | TWGCB-01-005-0170 | 安全性選項\使用者帳戶控制 | 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 | * 此原則設定會控制系統管理員之提升權限提示的行為，選項如下： * 提升權限而不提示：允許具有特殊權限的帳戶執行需要提升權限的操作，而不需同意或是認證。注意：請只在最嚴謹的環境中使用此選項 * 在安全桌面提示輸入認證：當操作需要提升權限時，會在安全桌面提示使用者輸入具有特殊權限的使用者名稱與密碼。如果使用者輸入有效的認證，操作會以使用者的最高可用權限繼續 * 在安全桌面提示要求同意：當操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 提示輸入認證：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 提示要求同意：當操作需要提升權限時，會提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 提示要求同意非Windows二進位檔案：(預設值)當非Microsoft應用程式的操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 | 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 | 在安全桌面提示要求同意 | CCE-ID：CCE-43921-6 |
| 171 | Windows10 Computer Settings | TWGCB-01-005-0171 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：標準使用者之提高權限提示的行為 | * 此項原則設定會控制標準使用者之提升權限提示的行為，選項如下： * 提示輸入認證(預設值)：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。若使用者輸入有效的認證，該操作會以適用的權限繼續執行 * 自動拒絕提升權限要求：當操作需要提升權限時，會顯示拒絕存取錯誤訊息。以標準使用者身分執行桌上型電腦的機關可能會選擇此設定，以降低需要尋求支援部門協助的機會 * 在安全桌面提示輸入認證：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。如果使用者輸入有效的認證，操作會以適用的權限繼續執行 | 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：標準使用者之提高權限提示的行為 | 在安全桌面提示輸入認證 | CCE-ID：CCE-43671-7 |
| 172 | Windows10 Computer Settings | TWGCB-01-005-0172 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：偵測應用程式安裝，並提示提升權限 | * 此項原則設定會控制電腦的應用程式安裝偵測行為，選項如下： * 啟用(預設值)：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。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 停用：未偵測到應用程式安裝封裝，也未提示提升權限。執行標準使用者桌面並利用委派安裝技術(例如，群組原則軟體安裝或Systems Management Server (SMS))的機關，應該停用此原則設定。在此情況下，不需要進行安裝程式偵測 | 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 | 啟用 | CCE-ID：CCE-43913-3 |
| 173 | Windows10 Computer Settings | TWGCB-01-005-0173 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：僅針對已簽署與驗證過的可執行檔，提升其權限 | * 此項原則設定將強制公開金鑰基礎結構(PKI)簽章檢查任何要求提升權限的互動式應用程式。系統管理員可透過將憑證新增至本機電腦的受信任的發行者憑證存放區，來控制允許執行哪些應用程式，選項如下： * 啟用：允許指定的可執行檔執行之前，強制執行PKI憑證路徑驗證 * 停用：允許指定的可執行檔執行之前，不強制執行PKI憑證路徑驗證 | 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：僅針對已簽署與驗證過的可執行檔，提升其權限 | 停用 | CCE-ID：CCE-43744-2 |
| 174 | Windows10 Computer Settings | TWGCB-01-005-0174 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：僅針對在安全位置安裝的UIAccess應用程式，提高其權限 | * 此項原則設定會控制要求以使用者介面協助工具(UIAccess)整合層級執行的應用程式必須位於檔案系統中的安全位置。安全位置僅限於下列目錄： * …\ProgramFiles\，包含子目錄 * …\Windows\system32\ * …\ProgramFiles(x86)\，包含64位元Windows版本的子目錄 * 注意：不論此項原則設定的狀態為何，Windows都會針對任何要求以UIAccess整合層級執行的互動式應用程式，強制執行公開金鑰基礎結構(PKI)簽章檢查，選項如下： * 啟用：如果應用程式位於檔案系統的安全位置，只會以UIAccess整合執行 * 停用：即使應用程式不是位於檔案系統的安全位置，也會以UIAccess整合執行 | 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：僅針對在安全位置安裝的UIAccess應用程式，提高其權限 | 啟用 | CCE-ID：CCE-42311-1 |
| 175 | Windows10 Computer Settings | TWGCB-01-005-0175 | 安全性選項\使用者帳戶控制 | 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 | * 此項原則設定會控制電腦的所有使用者帳戶控制(UAC)原則設定行為。如果變更此原則設定，必須重新啟動電腦，選項如下： * 已啟用(預設值)：啟用管理員核准模式。必須啟用此原則，而且必須以適當的方式設定相關的UAC原則設定，才能允許內建的Administrator帳戶以及所有其他屬於Administrators群組成員的使用者在管理員核准模式中執行 * 已停用：會停用管理員核准模式及所有相關的UAC原則設定。注意：如果停用此原則設定，資訊安全中心會通知您作業系統的整體安全性已降低 | 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 | 啟用 | CCE-ID：CCE-42995-1 |
| 176 | Windows10 Computer Settings | TWGCB-01-005-0176 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：提示提升權限時切換到安全桌面 | * 此項原則設定會控制提升權限要求提示是顯示在互動式使用者桌面或是安全桌面，選項如下： * 啟用：不論系統管理員與標準使用者的提示行為原則設定為何，所有提升權限要求都會顯示在安全桌面上 * 停用：所有提升權限要求都會顯示在互動式使用者桌面，並套用系統管理員與標準使用者的提示行為原則設定 | 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：提示提升權限時切換到安全桌面 | 啟用 | CCE-ID：CCE-41682-6 |
| 177 | Windows10 Computer Settings | TWGCB-01-005-0177 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置 | * 此項原則設定會控制是否將應用程式寫入失敗重新導向到已定義的登錄和檔案系統位置 * 此項原則設定可減少那些以系統管理員身分執行，並將執行階段應用程式資料寫入至%ProgramFiles%、%Windir%、%Windir%\system32或HKLM\Software的應用程式，選項如下： * 啟用：在執行階段將應用程式寫入失敗重新導向到檔案系統與登錄中已定義的使用者位置 * 停用：將資料寫入至受保護位置的應用程式失敗 | 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：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置 | 啟用 | CCE-ID：CCE-42858-1 |
| 178 | Windows10 Computer Settings | TWGCB-01-005-0178 | 使用者權限指派 | 從網路存取這台電腦 | * 此使用者權限決定允許哪些使用者與群組透過網路連線到這台電腦 * 遠端桌面服務不受此使用者權限的影響 | 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 | Administrators | CCE-ID：CCE-41806-1 |
| 179 | Windows10 Computer Settings | TWGCB-01-005-0179 | 使用者權限指派 | 當成作業系統的一部分 | * 此使用者權限可讓處理程序模擬任何使用者，而無需驗證。因此處理程序就可以取得與該使用者相同的本機資源存取權 * 需要此特殊權限的處理程序應使用LocalSystem帳戶(其已包括此特殊權限)，而不應使用其他特別指派此特殊權限的使用者帳戶 * 注意：指派此使用者權限可能會危及安全性。請僅將此使用者權限指派給信任的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\當成作業系統的一部分 | No One | CCE-ID：CCE-44315-0 |
| 180 | Windows10 Computer Settings | TWGCB-01-005-0180 | 使用者權限指派 | 調整處理程序的記憶體配額 | * 此特殊權限決定能變更處理程序可使用的最大記憶體的人員 * 注意：此特殊權限有助於系統調整，但可能會被濫用，例如阻斷服務攻擊 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\調整處理程序的記憶體配額 | Administrators, Local Service, Network Service | CCE-ID：CCE-43331-8 |
| 181 | Windows10 Computer Settings | TWGCB-01-005-0181 | 使用者權限指派 | 允許本機登入 | * 此使用者權限決定哪些使用者可以登入電腦 * 注意：修改此設定可能會影響用戶端、服務及應用程式的相容性 | 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 | Administrators, Users | CCE-ID：CCE-44186-5 |
| 182 | Windows10 Computer Settings | TWGCB-01-005-0182 | 使用者權限指派 | 允許透過遠端桌面服務登入 | 此項原則設定決定哪些使用者或群組擁有以遠端桌面服務用戶端登入的權限 | 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 | Remote Desktop Users, Administrators | CCE-ID：CCE-41832-7 |
| 183 | Windows10 Computer Settings | TWGCB-01-005-0183 | 使用者權限指派 | 備份檔案及目錄 | * 此使用者權限決定哪些使用者可以出於備份系統的目的，略過檔案及目錄、登錄及其他持續物件權限 * 具體而言，此使用者權限類似於將系統上所有檔案及資料夾的下列權限授與相關的使用者或群組： * 周遊資料夾/執行檔案 * 列出資料夾/讀取資料 * 讀取屬性 * 讀取擴充屬性 * 讀取權限 * 警告：指派此使用者權限可能會危及安全性。由於沒有方法可確定使用者是否正在備份資料、竊取資料或複製要發行的資料，因此請只將此使用者權限指派給受信任的使用者 * 在工作站及伺服器上的預設值： * Administrators * Backup Operators * 在網域控制站上的預設值 * Administrators * Backup Operators * Server Operators | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\備份檔案及目錄 | Administrators | CCE-ID：CCE-43438-1 |
| 184 | Windows10 Computer Settings | TWGCB-01-005-0184 | 使用者權限指派 | 略過周遊檢查 | * 此使用者權限決定哪些使用者即使沒有周遊目錄的權限，也能夠周遊目錄樹狀結構 * 此特殊權限不允許使用者列出目錄的內容，而只能周遊目錄 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\略過周遊檢查 | Administrators, Local Service, Network Service, Users | CCE-ID：CCE-43322-7 |
| 185 | Windows10 Computer Settings | TWGCB-01-005-0185 | 使用者權限指派 | 變更系統時間 | * 此使用者權限決定哪些使用者與群組能夠變更電腦內部時鐘的時間和日期 * 已指派此使用者權限的使用者可決定事件記錄檔的外觀。如果系統時間遭到變更，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 | 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 | Administrators, Local Service | CCE-ID：CCE-43011-6 |
| 186 | Windows10 Computer Settings | TWGCB-01-005-0186 | 使用者權限指派 | 變更時區 | * 此使用者權限決定哪些使用者與群組可以變更電腦顯示本地時間時使用的時區，也就是指電腦的系統時間加時差 * 系統時間本身是絕對的，而且不受時區變更的影響 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\變更時區 | Administrators, Local Service, Users | CCE-ID：CCE-42703-9 |
| 187 | Windows10 Computer Settings | TWGCB-01-005-0187 | 使用者權限指派 | 建立權杖物件 | * 此項原則設定決定處理程序可使用哪些帳戶來建立權杖，然後在處理程序使用內部應用程式開發介面(API)來建立存取權杖時，用以取得任何本機資源的存取權 * 此使用者權限是由作業系統內部使用。除非有此必要，否則不要將此使用者權限指派給Local System以外的使用者、群組或處理程序 * 注意：指派此使用者權限可能會危及安全性。不要將此使用者權限指派給不想由其掌控系統的任何使用者、群組或處理程序 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\建立權杖物件 | No One | CCE-ID：CCE-43249-2 |
| 188 | Windows10 Computer Settings | TWGCB-01-005-0188 | 使用者權限指派 | 建立通用物件 | * 此項原則設定決定使用者是否可以建立所有工作階段可用的全域物件。如果使用者沒有此使用者權限，仍然可以建立自己工作階段專用的物件 * 可以建立全域物件的使用者可能會影響其他使用者工作階段的程序，因而可能導致應用程式失敗或資料損毀 * 注意：指派此使用者權限可能會危及安全性。請只將此使用者權限指派給信任的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\建立通用物件 | Administrators, Local Service, Network Service, Service | CCE-ID：CCE-41605-7 |
| 189 | Windows10 Computer Settings | TWGCB-01-005-0189 | 使用者權限指派 | 建立永久共用物件 | * 此使用者權限決定哪些帳戶處理程序可以使用物件管理員來建立目錄物件 * 此使用者權限是由作業系統內部使用，且有助於延伸物件命名空間。因為此使用者權限已經指派給在核心模式下執行的元件，所以不需要特別指派 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\建立永久共用物件 | No One | CCE-ID：CCE-44313-5 |
| 190 | Windows10 Computer Settings | TWGCB-01-005-0190 | 使用者權限指派 | 建立符號連結 | * 此使用者權限會決定使用者是否可以從登入的電腦建立符號連結 * 注意： * 此特殊權限僅能授與信任的使用者。在並非設計來處理符號連結的應用程式中，符號連結會導致安全性風險 * 此設定可搭配symlink file system設定使用，透過使用命令列公用程式來控制電腦上允許的symlinks類型 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\建立符號連結 | Administrators | CCE-ID：CCE-42069-5 |
| 191 | Windows10 Computer Settings | TWGCB-01-005-0191 | 使用者權限指派 | 偵錯程式 | * 此使用者權限決定哪些使用者可將偵錯工具附加到任何處理程序或核心，可對機密且關鍵的作業系統元件提供完整存取權 * 不需要將此使用者權限指派給對自行開發的應用程式進行偵錯的開發人員。但開發人員需要此使用者權限，才能對新的系統元件進行偵錯 * 注意：指派此使用者權限可能會危及安全性。只將此使用者權限指派給信任的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\偵錯程式 | Administrators | CCE-ID：CCE-44192-3 |
| 192 | Windows10 Computer Settings | TWGCB-01-005-0192 | 使用者權限指派 | 拒絕從網路存取這台電腦 | * 此項原則設定決定會阻止哪些使用者從網路存取電腦 * 如果使用者帳戶同時受限於「拒絕從網路存取這台電腦」與「從網路存取這台電腦」這兩種原則，則此項原則設定會取代「從網路存取這台電腦」原則設定 | 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 | NT AUTHORITY\Local Account,  Guests | CCE-ID：CCE-42621-3 |
| 193 | Windows10 Computer Settings | TWGCB-01-005-0193 | 使用者權限指派 | 拒絕以批次工作登入 | * 此項原則設定決定會阻止哪些帳戶以批次工作登入 * 如果使用者帳戶同時受限於「拒絕以批次工作登入」與「以批次工作登入」這兩種原則，則此項原則設定會取代「以批次工作登入」原則設定 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\拒絕以批次工作登入 | Guests | CCE-ID：CCE-43428-2 |
| 194 | Windows10 Computer Settings | TWGCB-01-005-0194 | 使用者權限指派 | 拒絕以服務方式登入 | * 此項原則設定決定會阻止哪些服務帳戶以服務方式登錄處理程序 * 如果帳戶同時受限於「拒絕以服務方式登入」與「以服務方式登入」這兩種原則，則此項原則設定會取代「以服務方式登入」原則設定 * 注意：此項原則設定不適用於System、Local Service或Network Service帳戶 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\拒絕以服務方式登入 | Guests | CCE-ID：CCE-44172-5 |
| 195 | Windows10 Computer Settings | TWGCB-01-005-0195 | 使用者權限指派 | 拒絕本機登入 | * 此項原則設定決定將阻止哪些使用者登入電腦 * 如果帳戶同時受限於「拒絕本機登入」與「允許本機登入」這兩種原則，則此項原則設定會取代「允許本機登入」原則設定 * 注意：如果將此原則設定套用到Everyone群組，將無人可登入本機 | 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 | Guests | CCE-ID：CCE-43854-9 |
| 196 | Windows10 Computer Settings | TWGCB-01-005-0196 | 使用者權限指派 | 拒絕透過遠端桌面服務登入 | 此項原則設定決定會禁止哪些使用者與群組以遠端桌面服務用戶端登入 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\拒絕透過遠端桌面服務登入 | NT AUTHORITY\Local Account, Guests | CCE-ID：CCE-43886-1 |
| 197 | Windows10 Computer Settings | TWGCB-01-005-0197 | 使用者權限指派 | 讓電腦及使用者帳戶受信賴，以進行委派 | * 此原則設定決定哪些使用者可以在使用者或電腦物件上設定「信任委派」設定 * 擁有此特殊權限的使用者或物件，亦須擁有對使用者或電腦物件之帳戶控制旗標的寫入存取權。在被信任以便進行委派的電腦上(或在使用者環境下)，所執行的伺服器處理程序可透過用戶端的委派認證來存取另一台電腦的資源，前提是用戶端帳戶不能有「無法委派帳戶」帳戶控制旗標設定 * 此使用者權限會定義在「預設網域控制站群組原則」物件(GPO)及工作站、伺服器的本機安全性原則中 * 警告：濫用此使用者權限或「信任委派」設定，會造成網路非常容易受到特洛伊木馬程式的攻擊;此程式會模擬連入用戶端，並使用其認證，取得對網路資源的存取權 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\讓電腦及使用者帳戶受信賴，以進行委派 | No one | CCE-ID：CCE-43454-8 |
| 198 | Windows10 Computer Settings | TWGCB-01-005-0198 | 使用者權限指派 | 強制從遠端系統進行關閉 | * 此項原則設定決定哪些使用者能夠從網路上的遠端位置將電腦關機 * 濫用此使用者權限會造成阻斷服務 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\強制從遠端系統進行關閉 | Administrators | CCE-ID：CCE-42847-4 |
| 199 | Windows10 Computer Settings | TWGCB-01-005-0199 | 使用者權限指派 | 產生安全性稽核 | * 此項原則設定決定處理程序可使用哪些帳戶將項目新增到安全性記錄 * 安全性記錄檔是用來追蹤未經授權的系統存取。如果啟用「稽核：當無法記錄安全性稽核時，系統立即關機」安全性原則設定，濫用此使用者權限會導致產生許多稽核事件、可能會隱藏攻擊的辨識項，或造成阻斷服務 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\產生安全性稽核 | Local Service, Network Service | CCE-ID：CCE-41566-1 |
| 200 | Windows10 Computer Settings | TWGCB-01-005-0200 | 使用者權限指派 | 在驗證後模擬用戶端 | * 將此特殊權限指定給使用者可讓代表該使用者執行的程式模擬用戶端。要求此使用者權限以進行此類模擬，可防止未經授權的使用者說服用戶端連接(例如，透過遠端程序呼叫(RPC)或具名管道)至他們所建立的服務然後模擬該用戶端，進而避免將未授權使用者的權限提升到管理或系統層級 * 注意：指派此使用者權限可能會危及安全性。請僅將此使用者權限指派給信任的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\在驗證後模擬用戶端 | Administrators, Local Service, Network Service, Service | CCE-ID：CCE-43050-4 |
| 201 | Windows10 Computer Settings | TWGCB-01-005-0201 | 使用者權限指派 | 增加處理程序工作組 | * 此權限決定哪些使用者帳戶可以增加或減少處理程序的工作組大小 * 處理程序的工作組是實體RAM記憶體中的處理程序目前可見的記憶體頁面組。這些頁面是常駐的，且可讓應用程式使用而不會觸發分頁錯誤。工作組的大小下限與上限可以影響處理程序的虛擬記憶體分頁行為 * 注意：增加處理程序的工作組大小會減少系統其他部分可用的實體記憶體總數 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\增加處理程序工作組 | Administrators, Local Service | CCE-ID：CCE-44298-8 |
| 202 | Windows10 Computer Settings | TWGCB-01-005-0202 | 使用者權限指派 | 增加排程優先順序 | * 此項原則設定決定哪些帳戶能使用具有寫入內容的處理程序存取其他處理程序，來增加指派給其他處理程序的執行優先順序 * 具有此特殊權限的使用者能夠透過「工作管理員」使用者介面來變更處理程序的排程優先順序 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\增加排程優先順序 | Administrators | CCE-ID：CCE-41771-7 |
| 203 | Windows10 Computer Settings | TWGCB-01-005-0203 | 使用者權限指派 | 載入及解除載入裝置驅動程式 | * 此使用者權限決定哪些使用者能在核心模式中動態載入與解除載入裝置驅動程式或其他程式碼 * 此使用者權限不適用於隨插即用裝置驅動程式 * 注意：指派此使用者權限可能會危及安全性。不要將此使用者權限指派給不想由其掌控系統的任何使用者、群組或處理程序 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\載入及解除載入裝置驅動程式 | Administrators | CCE-ID：CCE-42840-9 |
| 204 | Windows10 Computer Settings | TWGCB-01-005-0204 | 使用者權限指派 | 存取認證管理員作為信任的呼叫者 | 在備份/還原時，認證管理員會使用此設定。帳戶不應該擁有此權限，因為它只會被指派給Winlogon。如果此權限指定給其他實體，則使用者儲存的認證可能會被洩露 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\存取認證管理員作為信任的呼叫者 | No one | CCE-ID：CCE-43917-4 |
| 205 | Windows10 Computer Settings | TWGCB-01-005-0205 | 使用者權限指派 | 鎖定記憶體中的分頁 | * 此項原則設定決定哪些使用者能使用處理程序來保留實體記憶體中的資料，阻止系統將資料分頁到磁碟上的虛擬記憶體 * 執行此特殊權限會降低可用的隨機存取記憶體(RAM)數量，對系統效能造成顯著影響 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\鎖定記憶體中的分頁 | No One | CCE-ID：CCE-43750-9 |
| 206 | Windows10 Computer Settings | TWGCB-01-005-0206 | 使用者權限指派 | 以批次工作登入 | 此項原則設定允許使用者以批次佇列設備登入，且僅提供與舊版Windows相容之用，例如：當使用者以工作排程器提交工作時，工作排程器會以批次使用者登入該使用者，而不是互動式使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\以批次工作登入 | No One | CCE-ID：CCE-43615-4 |
| 207 | Windows10 Computer Settings | TWGCB-01-005-0207 | 使用者權限指派 | 以服務方式登入 | * 此項原則設定可以允許安全性主體以服務方式登入 * 服務可以設定成以Local System、Local Service或Network Service帳戶執行，這些帳戶具有內建權限可以服務方式登入。任何以個別的使用者帳戶執行的服務都必須被指派此權限 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\以服務方式登入 | No One | CCE-ID：CCE-44370-5 |
| 208 | Windows10 Computer Settings | TWGCB-01-005-0208 | 使用者權限指派 | 管理稽核及安全性記錄檔 | * 此項原則設定決定哪些使用者能夠指定個別資源(例如：檔案、Active Directory物件和登錄機碼)的物件存取稽核選項 * 此項原則設定禁止使用者啟用檔案與物件存取稽核。如需啟用這類稽核，便必須設定「電腦設定\Windows設定\安全性設定\本機原則\稽核原則」中的「稽核物件存取」設定 * 使用者可以在事件檢視器的安全性記錄檔中檢視稽核的事件。具有此特殊權限的使用者也可以檢視與清除安全性記錄檔 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\管理稽核及安全性記錄檔 | Administrators | CCE-ID：CCE-41974-7 |
| 209 | Windows10 Computer Settings | TWGCB-01-005-0209 | 使用者權限指派 | 修改物件標籤 | * 此特殊權限可決定哪些使用者帳戶可修改物件(例如：檔案、登錄機碼或由其他使用者擁有的處理程序)的完整性標籤 * 在使用者帳戶下執行的處理程序不需要此特殊權限，即可修改該使用者擁有之物件的標籤 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\修改物件標籤 | No One | CCE-ID：CCE-44133-7 |
| 210 | Windows10 Computer Settings | TWGCB-01-005-0210 | 使用者權限指派 | 修改韌體環境值 | * 此項原則設定決定何人可以修改韌體環境值。韌體環境變數是存放在非x86型電腦之非揮發性RAM中的設定。設定的效果需視處理器而定 * 在x86型電腦上，可以透過指派這個使用者權限而修改的唯一韌體環境值是「上次的正確設定」，而這應該只由系統修改 * 在Itanium型電腦上，開機資訊是儲存在非揮發性RAM中。必須將此使用者權限指派給使用者，使用者才能執行bootcfg.exe及變更「系統內容」中「啟動及修復」上的「預設作業系統」設定 * 在所有的電腦上，安裝或升級Windows都需要此使用者權限 * 注意：此項原則設定不會影響能修改系統環境變數及使用者環境變數(位於「系統內容」的「進階」索引標籤)的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\修改韌體環境值 | Administrators | CCE-ID：CCE-44295-4 |
| 211 | Windows10 Computer Settings | TWGCB-01-005-0211 | 使用者權限指派 | 執行磁碟區維護工作 | * 此項原則設定決定哪些使用者與群組能在磁碟區上執行維護工作，例如遠端磁碟重組 * 指派此使用者權限時要特別小心。具有此使用者權限的使用者可以瀏覽磁碟和將檔案延伸到包含其他資料的記憶體中。當延伸檔案開啟時，使用者能夠讀取和修改取得的資料 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\執行磁碟區維護工作 | Administrators | CCE-ID：CCE-43381-3 |
| 212 | Windows10 Computer Settings | TWGCB-01-005-0212 | 使用者權限指派 | 監視單一處理程序 | 此項原則設定決定哪些使用者可使用效能監視工具來監視「非」系統處理程序的效能 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\監視單一處理程序 | Administrators | CCE-ID：CCE-44136-0 |
| 213 | Windows10 Computer Settings | TWGCB-01-005-0213 | 使用者權限指派 | 監視系統效能 | 此項原則設定決定哪些使用者可使用效能監視工具來監視系統處理程序的效能 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\監視系統效能 | Administrators, WdiServiceHost | CCE-ID：CCE-42247-7 |
| 214 | Windows10 Computer Settings | TWGCB-01-005-0214 | 使用者權限指派 | 取代處理程序等級權杖 | * 此項原則設定決定哪些使用者帳戶能夠呼叫CreateProcessAsUser()應用程式開發介面(API)，使得一個服務能夠啟動另一個服務 * 工作排程器是應用此使用者權限的處理程序的範例之一 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\取代處理程序等級權杖 | Local Service, Network Service | CCE-ID：CCE-43648-5 |
| 215 | Windows10 Computer Settings | TWGCB-01-005-0215 | 使用者權限指派 | 還原檔案及目錄 | * 此項原則設定決定哪些使用者可以在還原備份檔案及目錄時，略過檔案、目錄、登錄及其他持續物件的權限，並決定哪些使用者可以物件擁有者的身分，設定任何有效的安全性主體 * 這項使用者權限類似於將系統上所有檔案及資料夾的下列權限授予相關的使用者或群組： * 周遊資料夾/執行檔案 * 寫入 * 注意：指派此使用者權限可能會危及安全性。由於擁有使用者權限的使用者可以覆寫登錄設定、隱藏資料及取得系統物件的所有權，請僅指派這個使用者權限給信任的使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\還原檔案及目錄 | Administrators | CCE-ID：CCE-42133-9 |
| 216 | Windows10 Computer Settings | TWGCB-01-005-0216 | 使用者權限指派 | 關閉系統 | * 此項原則設定決定哪些本機登入電腦的使用者能夠使用Shutdown命令將作業系統關機 * 濫用此使用者權限將可能造成阻斷服務 | 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 | Administrators, Users | CCE-ID：CCE-44284-8 |
| 217 | Windows10 Computer Settings | TWGCB-01-005-0217 | 使用者權限指派 | 取得檔案或其他物件的擁有權 | * 此項原則設定決定哪些使用者能夠取得系統中任何安全物件的擁有權，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 * 注意：指派此使用者權限可能會危及安全性。由於物件擁有者將會擁有完全控制，請將此使用者權限僅指派給信任的使用者 | 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 | Administrators | CCE-ID：CCE-41977-0 |
| 218 | Windows10 Computer Settings | TWGCB-01-005-0218 | 使用者權限指派 | 同步處理目錄服務資料 | 此項原則設定決定授權哪些使用者及群組同步處理所有目錄服務資料，此項原則設定亦稱為Active Directory同步處理 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\同步處理目錄服務資料 | No One | CCE-ID：CCE-42451-5 |
| 219 | Windows10 Computer Settings | TWGCB-01-005-0219 | 使用者權限指派 | 建立分頁檔 | * 此使用者權限決定哪些使用者及群組能夠呼叫內部應用程式開發介面(API)來建立分頁檔及變更其大小。此使用者權限是由作業系統內部使用且通常不需要指派給任何使用者 * 如需有關如何為指定的磁碟機指定分頁檔大小的詳細資訊，請參閱「變更虛擬記憶體分頁檔的大小」 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\建立分頁檔 | Administrators | CCE-ID：CCE-42381-4 |
| 220 | Windows10 Computer Settings | TWGCB-01-005-0220 | Windows元件 | 防止精靈執行 | * 根據預設，所有系統管理員都可以使用新增功能到Windows 10 * 如果啟用此項原則設定，就不會執行精靈 * 如果停用此項原則設定或將它設為「尚未設定」，則會執行精靈 | 電腦設定\系統管理範本\Windows元件\新增功能到Windows 10\防止精靈執行 | 啟用 | CCE-ID：CCE-41675-0 |
| 221 | Windows10 Computer Settings | TWGCB-01-005-0221 | Windows元件 | 允許選用Microsoft 帳戶 | * 此項原則設定可控制需要帳戶登入的Windows市集應用程式是否可以選用Microsoft帳戶。此項原則只會影響支援該功能的Windows市集應用程式 * 如果啟用此項原則設定，通常需要Microsoft帳戶登入的Windows市集應用程式，將允許使用者改用企業帳戶登入 * 如果停用或未設定此項原則設定，則使用者必須使用Microsoft帳戶登入 | 電腦設定\系統管理範本\Windows元件\應用程式執行階段\允許選用 Microsoft帳戶 | 啟用 | CCE-ID：CCE-44037-0 |
| 222 | Windows10 Computer Settings | TWGCB-01-005-0222 | Windows元件 | 關閉自動播放 | * 此項原則設定決定是否關閉自動播放功能 * 當使用者將媒體插入磁碟機時，自動播放會立即開始讀取該磁碟機。如此一來，程式的安裝檔案和音訊媒體上的音樂便會立即啟動 * 如果啟用此項原則設定，即會停用光碟機及抽取式媒體磁碟機上的自動播放，或停用所有磁碟機的自動播放功能 * 此項設定會停用其他類型磁碟機上的自動播放功能如果磁碟機上的自動播放功能預設是停用的，使用者就無法使用此項設定來啟用該功能 * 注意：此項設定會同時出現在「電腦設定」及「使用者設定」資料夾中。如果這兩處的設定相衝突，則「電腦設定」中之設定的優先順序會高於「使用者設定」中的設定 | 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 | 啟用，所有磁碟機 | CCE-ID：CCE-43848-1 |
| 223 | Windows10 Computer Settings | TWGCB-01-005-0223 | Windows元件 | 設定AutoRun的預設行為 | * 此項原則設定可設定Auto Run命令的預設行為 * 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常式 * 在Windows Vista之前，在插入含有AutoRun命令的媒體時，系統會自動執行程式，而不需使用者介入 * 這會產生主要的安全性考量，因為程式碼可能會在使用者不知情的情況下執行。從Windows Vista開始的預設行為是，提示使用者是否要執行AutoRun命令 * Auto Run命令會呈現為「自動播放」對話方塊中的處理常式 * 如果啟用此項原則設定，系統管理員可以將Windows Vista或更新版本的AutoRun預設行為變更為下列行為： * 完全停用AutoRun命令，或者 * 轉換回Windows Vista之前的行為，自動執行AutoRun命令 * 如果停用或未設定此項原則設定，Windows Vista或更新版本將會提示使用者是否要執行AutoRun命令 | 電腦設定\系統管理範本\Windows元件\自動播放原則\設定Autorun的預設行為 | 啟用，不執行任何AutoRun命令 | CCE-ID：CCE-41501-8 |
| 224 | Windows10 Computer Settings | TWGCB-01-005-0224 | Windows元件 | 不允許非磁碟區裝置的自動播放 | * 此項原則設定不允許MTP裝置(如相機或電話)的自動播放 * 如果啟用此項原則設定，將不允許MTP裝置(如相機或電話)的自動播放 * 如果停用或未設定此項原則設定，將可啟用非磁碟區裝置的自動播放 | 電腦設定\系統管理範本\Windows元件\自動播放原則\不允許非磁碟區裝置的自動播放 | 啟用 | CCE-ID：CCE-41844-2 |
| 225 | Windows10 Computer Settings | TWGCB-01-005-0225 | Windows元件 | 限制解壓縮和安裝未經過數位簽署的小工具 | * 此項原則設定決定是否限制安裝未經簽署的小工具。桌面小工具可部署為經過數位簽署或未經簽署的壓縮檔 * 如果啟用此項原則設定，未經過數位簽署的小工具不會解壓縮 * 如果停用或未做此項原則設定，則經過簽署與未簽署的小工具兩者都會解壓縮 | 電腦設定\系統管理範本\Windows元件\桌面小工具\限制解壓縮和安裝未經過數位簽署的小工具 | 啟用 | CCE-ID：CCE-42717-9 |
| 226 | Windows10 Computer Settings | TWGCB-01-005-0226 | Windows元件 | 關閉使用者安裝的桌面小工具 | * 此項原則設定可讓關閉已由使用者安裝的桌面小工具 * 如果啟用此原則設定，Windows不會執行任何使用者安裝的小工具 * 如果停用或未設定此原則設定，則Windows會執行使用者安裝的小工具。Windows預設為會執行使用者安裝的小工具 | 電腦設定\系統管理範本\Windows元件\桌面小工具\關閉使用者安裝的桌面小工具 | 啟用 | CCE-ID：CCE-43471-2 |
| 227 | Windows10 Computer Settings | TWGCB-01-005-0227 | Windows元件 | 關閉桌面小工具 | * 此項原則設定決定是否關閉桌面小工具。桌面小工具是在桌面上顯示資訊或公用程式的小程式 * 如果啟用此項原則設定，將會關閉桌面小工具 * 如果停用或未設定此項原則設定，則會開啟桌面小工具 | 電腦設定\系統管理範本\Windows元件\桌面小工具\關閉桌面小工具 | 啟用 | CCE-ID：CCE-41519-0 |
| 228 | Windows10 Computer Settings | TWGCB-01-005-0228 | Windows元件 | 停用記錄 | * 此項原則設定決定是否將「Windows錯誤報告」事件記錄到系統事件日誌中 * 如果此項原則設定已啟用，則「Windows錯誤報告」事件將不會記錄到系統事件日誌 * 如果停用或未設定此項原則設定，則Windows錯誤報告事件和錯誤會記錄在系統事件日誌中(與其他Windows程式一起) | 電腦設定\系統管理範本\Windows元件\ Windows錯誤報告\停用記錄 | 停用 | CCE-ID：CCE-43330-0 |
| 229 | Windows10 Computer Settings | TWGCB-01-005-0229 | Windows元件 | 停用Windows錯誤報告 | * 此項原則設定會關閉Windows錯誤報告，因此當軟體發生未預期的停止或失敗時，不會收集或傳送報告給Microsoft或機關內的內部伺服器 * 如果啟用此項原則設定，Windows錯誤報告不會傳送任何問題資訊到Microsoft。此外，「控制台中的」的「安全性與維護」不會提供解決方案 * 如果停用或未設定此項原則設定，則「電腦設定/系統管理範本/系統/網際網路通訊管理/網際網路通訊/關閉Windows錯誤報告」原則設定的優先順序最高 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\停用Windows錯誤報告 | 啟用 | CCE-ID：CCE-44385-3 |
| 230 | Windows10 Computer Settings | TWGCB-01-005-0230 | Windows元件 | 不傳送其他資料 | * 此項原則設定決定支援錯誤報告的其他資料是否可以自動傳送到Microsoft * 如果啟用此項原則設定，則不會通知使用者而自動拒絕回應「Windows錯誤報告」事件時Microsoft所要求的任何其他資料 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\不傳送其他資料 | 啟用 | CCE-ID：CCE-44381-2 |
| 231 | Windows10 Computer Settings | TWGCB-01-005-0231 | Windows元件 | 顯示錯誤通知 | * 此項原則設定可以控制是否向使用者顯示讓他們報告錯誤的錯誤對話方塊 * 如果啟用此項原則設定，系統會以對話方塊通知使用者發生錯誤，並顯示更多與錯誤相關的詳細資料 * 如果也啟用了「設定錯誤報告」原則設定，使用者便可以報告錯誤 * 如果停用此項原則設定，使用者將無法收到發生錯誤的通知。如果同時啟用了「設定錯誤報告」原則設定，則會報告錯誤，但使用者不會收到通知。對於沒有互動使用者的伺服器來說，停用此項原則設定很實用 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\顯示錯誤通知 | 停用 | CCE-ID：CCE-43668-3 |
| 232 | Windows10 Computer Settings | TWGCB-01-005-0232 | Windows元件 | 關閉Windows Mail應用程式 | * 拒絕或允許存取此Windows郵件應用程式 * 如啟用此項原則設定，將拒絕存取Windows郵件應用程式 * 如停用或未設定此項原則設定，將允許存取Windows郵件應用程式 | 電腦設定\系統管理範本\Windows元件\Windows Mail\關閉Windows Mail應用程式 | 啟用 | 適用1709以前版本  CCE-ID：CCE-44098-2 |
| 233 | Windows10 Computer Settings | TWGCB-01-005-0233 | Windows元件 | 關閉社群功能 | Windows郵件不會替社群支援服務檢查的新聞群組伺服器 | 電腦設定\系統管理範本\Windows元件\Windows Mail\關閉社群功能 | 啟用 | 適用1709以前版本  CCE-ID：CCE-43160-1 |
| 234 | Windows10 Computer Settings | TWGCB-01-005-0234 | Windows元件 | 永遠以較高的特殊權限安裝 | * 此項原則設定會指定Windows Installer在安裝任何程式到系統時應使用較高的權限 * 如果啟用此項原則設定，會將特殊權限延伸到所有程式。這些特殊權限通常保留給已指派給使用者的程式(在桌面上提供)、已指派給電腦的程式(自動安裝)，或可以在「控制台」的「新增或移除程式」中使用的程式 * 此項設定檔設定可以讓使用者安裝某些程式，而這些程式需要存取的目錄可能是使用者沒有權限檢視或變更的目錄(包括位在高限制性電腦上的目錄) * 如果停用或未設定此項原則設定，則系統會在安裝不是由系統管理員分配或提供的程式時，套用目前使用者的使用權限 * 注意：此項原則設定會同時出現在「電腦設定」及「使用者設定」資料夾中。如果要讓此項原則設定生效，必須啟用上述兩個資料夾中的設定 * 警告：有經驗的使用者可能會利用此項原則設定所授與的使用權限，來變更他們的特殊權限並得以永久存取設限的檔案和資料夾。請注意，此項原則設定的「使用者設定」版本不保證是安全的 | 電腦設定\系統管理範本\Windows元件\Windows Installer\永遠以較高的特殊權限安裝 | 停用 | CCE-ID：CCE-42775-7 |
| 235 | Windows10 Computer Settings | TWGCB-01-005-0235 | Windows元件 | 允許使用者控制安裝 | * 此項原則設定決定是否允許使用者變更某些通常僅供系統管理員使用的安裝選項 * 如果此項原則設定為啟用，則會略過Windows Installer的部分安全性功能。它能讓安裝完成，不因安全性違規而暫停安裝 * 如果此項原則設定為停用或未設定，Windows Installer的安全性功能會防止使用者變更某些通常保留給系統管理員的安裝選項，例如指定檔案安裝目錄 * 如果Windows Installer偵測到某個安裝套裝軟體已允許使用者變更受保護的選項，它將會停止安裝並顯示訊息。只有當安裝程式是在可存取使用者被拒的目錄之特殊權限的安全性內容上執行時，這些安全性功能才能操作 * 此項設定是針對較少限制的環境而設計。它可以用來規避安裝程式中防止軟體被安裝的錯誤 | 電腦設定\系統管理範本\Windows元件\Windows Installer\允許使用者控制安裝 | 停用 | CCE-ID：CCE-44168-3 |
| 236 | Windows10 Computer Settings | TWGCB-01-005-0236 | Windows元件 | 禁止非系統管理員套用廠商簽署的更新 | * 此項原則設定控制非系統管理員是否可以安裝已經由應用程式廠商數位簽署的更新 * 如果啟用 此項原則設定，則只有系統管理員或擁有系統管理員權限的使用者才可以套用更新到以Windows Installer為基礎的應用程式 * 如果停用或未設定此項原則設定，則沒有系統管理員權限的使用者將可以安裝非系統管理員更新 | 電腦設定\系統管理範本\Windows元件\Windows Installer\禁止非系統管理員套用廠商簽署的更新 | 啟用 | CCE-ID：CCE-43300-3 |
| 237 | Windows10 Computer Settings | TWGCB-01-005-0237 | Windows元件 | 防止出現Windows Installer指令碼的Internet Explorer安全性提示 | * 此項原則設定決定是否允許以網頁為基礎的程式在電腦上安裝軟體時，不需要通知使用者 * 預設狀況下，當網際網路瀏覽器管理的指令碼嘗試將程式安裝到系統時，系統會警告使用者，並讓使用者選擇或拒絕安裝。此項設定會抑制警告，並允許安裝繼續進行 * 此設定是針對使用以網頁為基礎的工具來發布程式給員工的機關所設計。不過，由於此項設定可能有安全性風險，因此應該謹慎使用 | 電腦設定\系統管理範本\Windows元件\Windows Installer\防止出現Windows Installer指令碼的Internet Explorer安全性提示 | 停用 | CCE-ID：CCE-41982-0 |
| 238 | Windows10 Computer Settings | TWGCB-01-005-0238 | Windows元件 | 不要顯示「安裝第一次使用」對話方塊 | * 此項原則設定決定是否要顯示「安裝第一次使用」對話方塊 * 啟用此項原則時，在使用者第一次啟動Windows Media Player時，將不顯示「隱私權選項」與「安裝選項」對話方塊 * 如果未設定或已停用此項原則，就會在使用者第一次啟動Player時，顯示對話方塊 | 電腦設定\系統管理範本\Windows元件\Windows Media Player\不要顯示「安裝第一次使用」對話方塊 | 啟用 | CCE-ID：CCE-43178-3 |
| 239 | Windows10 Computer Settings | TWGCB-01-005-0239 | Windows元件 | 防止自動更新 | * 此項原則設定決定是否防止向使用者提示更新Windows Media Player，而且即使Player有可用的更新版本，具有系統管理員權限的使用者也不會看到更新的提示。Player中「說明」功能表上的「檢查是否有播放程式更新版」命令是無法使用的。此外，「播放程式」索引標籤上「檢查更新」區域中的時間間隔都未選取，也無法使用 * 如果未設定或已停用此項原則，則只有具系統管理員權限的使用者可以使用「檢查是否有播放程式更新版」，並且在有可用的更新版本時，他們便會看到更新提示。依照預設，具系統管理員權限的使用者可以選擇檢查更新的頻率 * 沒有系統管理員權限的使用者不會看到「檢查是否有播放程式更新版」，而且即使沒有此項原則，他們也不會看到更新提示 | 電腦設定\系統管理範本\Windows元件\Windows Media Player\防止自動更新 | 啟用 | CCE-ID：CCE-44026-3 |
| 240 | Windows10 Computer Settings | TWGCB-01-005-0240 | Windows元件 | 不要顯示密碼顯示按鈕 | * 此項原則設定可設定當使用者輸入密碼時，是否顯示密碼顯示按鈕 * 如果啟用此項原則設定，當使用者在密碼輸入文字方塊中輸入密碼後，就不會顯示密碼顯示按鈕 * 如果停用或未設定此項原則設定，當使用者在密碼輸入文字方塊中輸入密碼後，會顯示密碼顯示按鈕 * 根據預設，使用者在密碼輸入文字方塊中輸入密碼後，會顯示密碼顯示按鈕。若要顯示密碼，按一下密碼顯示按鈕 * 此項原則適用於所有使用Windows系統控制項的Windows元件和應用程式，包含Internet Explorer | 電腦設定\系統管理範本\Windows元件\認證使用者介面\不要顯示密碼顯示按鈕 | 啟用 | CCE-ID：CCE-42652-8 |
| 241 | Windows10 Computer Settings | TWGCB-01-005-0241 | Windows元件 | 提升權限時列舉系統管理員帳戶 | * 此項原則設定針對嘗試以提升的權限執行應用程式時，決定是否要顯示系統管理員帳戶 * 若啟用此原則設定，會顯示電腦上的所有本機系統管理員帳戶，以便使用者可以選擇系統管理員帳戶並輸入正確的密碼 * 若停用此原則設定，每次提升權限時都會要求使用者輸入使用者名稱與密碼 | 電腦設定\系統管理範本\Windows元件\認證使用者介面\提升權限時列舉系統管理員帳戶 | 停用 | CCE-ID：CCE-43619-6 |
| 242 | Windows10 Computer Settings | TWGCB-01-005-0242 | Windows元件 | 控制記錄檔達到其大小上限時的事件記錄檔行為(應用程式) | * 如果啟用此項原則設定，當記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失 * 如果停用或未設定此項原則設定，當記錄檔達到其大小上限，則新事件會覆寫舊事件 * 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定 | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\應用程式\控制記錄檔達到其大小上限時的事件記錄檔行為 | 停用 | CCE-ID：CCE-43472-0 |
| 243 | Windows10 Computer Settings | TWGCB-01-005-0243 | Windows元件 | 指定記錄檔大小上限(KB)(應用程式) | * 此原則設定可決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，此值預設為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\應用程式\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 | CCE-ID：CCE-41972-1 |
| 244 | Windows10 Computer Settings | TWGCB-01-005-0244 | Windows元件 | 控制記錄檔達到其大小上限時的事件記錄檔行為(安全性) | * 如果啟用此項原則設定，當記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失 * 如果停用或未設定此項原則設定，當記錄檔達到其大小上限，則新事件會覆寫舊事件 * 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定 | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安全性\控制記錄檔達到其大小上限時的事件記錄檔行為 | 停用 | CCE-ID：CCE-44139-4 |
| 245 | Windows10 Computer Settings | TWGCB-01-005-0245 | Windows元件 | 指定記錄檔大小上限(KB)(安全性) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安全性\指定記錄檔大小上限(KB) | 啟用，81,920KB以上 | CCE-ID：CCE-42340-0 |
| 246 | Windows10 Computer Settings | TWGCB-01-005-0246 | Windows元件 | 指定記錄檔大小上限(KB)(安裝) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安裝\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 | CCE-ID：CCE-44151-9 |
| 247 | Windows10 Computer Settings | TWGCB-01-005-0247 | Windows元件 | 控制記錄檔達到其大小上限時的事件記錄檔行為(系統) | * 如果啟用此項原則設定，當記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失 * 如果停用或未設定此項原則設定，當記錄檔達到其大小上限，則新事件會覆寫舊事件 * 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定 | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\系統\控制記錄檔達到其大小上限時的事件記錄檔行為 | 停用 | CCE-ID：CCE-43655-0 |
| 248 | Windows10 Computer Settings | TWGCB-01-005-0248 | Windows元件 | 指定記錄檔大小上限(KB)(系統) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\系統\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 | CCE-ID：CCE-41582-8 |
| 249 | Windows10 Computer Settings | TWGCB-01-005-0249 | Windows元件 | 不允許儲存密碼 | * 此項原則設定決定是否從遠端桌面連線將密碼儲存在這部電腦上。如果啟用此項原則設定，「遠端桌面連線」的密碼儲存核取方塊將會停用，而且使用者再也無法儲存密碼。當使用者使用遠端桌面連線開啟RDP檔案並儲存其設定後，所有先前存在於RDP檔案中的密碼都將予以刪除 * 如果停用或未設定此項原則設定，則使用者能夠使用遠端桌面連線儲存密碼 | 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 | 啟用 | CCE-ID：CCE-44410-9 |
| 250 | Windows10 Computer Settings | TWGCB-01-005-0250 | Windows元件 | 允許使用者使用遠端桌面服務從遠端連線 | * 此項原則設定決定是否讓使用者使用遠端桌面服務，設定電腦的遠端存取權 * 如果啟用此項原則設定，目標電腦上隸屬於Remote Desktop Users群組成員的使用者就可以使用遠端桌面服務，從遠端連線到目標電腦 * 如果停用此項原則設定，使用者無法使用遠端桌面服務，從遠端連線到目標電腦。目標電腦會保留任何目前的連線，但是不會接受任何新連入的連線 * 如果未設定此項原則設定，則遠端桌面服務會使用目標電腦上的「遠端桌面」設定，決定是否允許遠端連線 * 注意：使用者可以藉由設定「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\透過使用網路層級驗證以要求對遠端連線進行使用者驗證」原則設定，限制可以使用遠端桌面服務進行遠端連線的用戶端。使用者也可以限制可同時連線的使用者數量，方法是設定「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\限制連線數目」原則設定，或在遠端桌面工作階段主機設定工具的「網路介面卡」索引標籤上設定「連線數目上限」選項 | 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 | 停用 | CCE-ID：CCE-41772-5 |
| 251 | Windows10 Computer Settings | TWGCB-01-005-0251 | Windows元件 | 不允許磁碟重新導向 | * 此項原則設定指定在遠端桌面服務工作階段中，是否要防止對應用戶端磁碟機(磁碟機重新導向) * 根據預設，RD工作階段主機伺服器會在連線時自動對應用戶端磁碟機。對應的磁碟機會以「<磁碟機代號>於<電腦名稱>」的格式，顯示在「檔案總管」或電腦的工作階段資料夾樹狀目錄中。可以使用此項原則設定覆寫這種行為 * 如果啟用此項原則設定，就不允許在遠端桌面服務工作階段中，重新導向用戶端磁碟機 * 如果停用此項原則設定，就一律允許重新導向用戶端磁碟機。此外，如果允許剪貼簿重新導向，就永遠允許剪貼簿檔案複製重新導向 * 如果未設定此項原則設定，則不會在群組原則層級指定用戶端磁碟機重新導向和剪貼簿檔案複製重新導向 | 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\裝置及資源重新導向\不允許磁碟重新導向 | 啟用 | CCE-ID：CCE-44238-4 |
| 252 | Windows10 Computer Settings | TWGCB-01-005-0252 | Windows元件 | 連線時永遠提示密碼 | * 此項原則設定決定遠端桌面服務是否總是會在連線時，提示用戶端輸入密碼 * 使用者可以使用此項設定，對登入遠端桌面服務的使用者強制執行密碼提示，即使他們已經在遠端桌面連線用戶端中提供過密碼 * 遠端桌面服務預設為允許使用者在遠端桌面連線用戶端中輸入密碼即可自動登入 * 如果此項原則設定為「啟用」，使用者即使已經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。他們會收到要求輸入登入密碼的提示 * 如果此項原則設定為「停用」，使用者只要在遠端桌面連線用戶端中提供過密碼，就一律可以自動登入遠端桌面服務 * 如果此項原則設定為「尚未設定」，則不會於群組原則層級指定自動登入。不過，系統管理員仍然可以使用遠端桌面工作階段主機設定工具，強制執行密碼提示 | 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 | 啟用 | CCE-ID：CCE-43700-4 |
| 253 | Windows10 Computer Settings | TWGCB-01-005-0253 | Windows元件 | 設定用戶端連線加密層級 | * 此項原則設定決定在遠端桌面通訊協定(RDP)連線期間，是否必須使用特定的加密層級，來確保用戶端與RD工作階段主機伺服器之間的通訊安全 * 如果啟用此項原則設定，在遠端連線期間，用戶端與RD工作階段主機伺服器之間的所有通訊都必須使用此項設定中指定的加密方法。加密層級預設為「高等級」。可用的加密方法如下： * 高等級：設定「高等級」會使用增強式128位元加密，來加密從用戶端傳送至伺服器的資料，以及從伺服器傳送至用戶端的資料。請在只包含128位元用戶端(例如，執行遠端桌面連線的用戶端)的環境中使用這個加密層級。不支援這個加密層級的用戶端無法連線到RD工作階段主機伺服器 * 用戶端相容：設定「用戶端相容」會以用戶端支援的最大金鑰效力，加密用戶端與伺服器之間傳送的資料。請在包含不支援128位元加密之用戶端的環境中使用這個加密層級 * 低等級：設定「低等級」只會使用56位元加密，來加密從用戶端傳送至伺服器的資料 | 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 | 啟用，高等級 | CCE-ID：CCE-42894-6 |
| 254 | Windows10 Computer Settings | TWGCB-01-005-0254 | Windows元件 | 為使用中但閒置的遠端桌面服務工作階段設定時間限制 | * 此項原則設定決定使用中的遠端桌面服務工作階段在自動中斷連線之前可以閒置(沒有使用者輸入)的時間上限 * 如果啟用此項原則設定，使用者必須在「閒置工作階段限制」下拉式清單中選取想要的時間限制。經過指定的時間後，遠端桌面服務會自動中斷使用中但閒置之工作階段的連線。使用者會在工作階段中斷連線前兩分鐘收到警告訊息，讓他們可以按下按鍵或移動滑鼠，使工作階段保持使用中狀態。如果使用者有主控台工作階段，則不適用閒置工作階段的時間限制 * 如果停用或未設定此項原則設定，遠端桌面服務會允許工作階段無限期保持使用中但閒置狀態。使用者可以在遠端桌面工作階段主機設定工具的「工作階段」索引標籤上，指定使用中但閒置之工作階段的時間限制 * 如果要在到達時間限制時讓遠端桌面服務終止工作階段而非中斷連線，可以設定「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\超過使用時間限制就結束工作階段」原則設定 * 注意：此項原則設定同時出現在「電腦設定」和「使用者設定」中。如果兩個原則都已設定，「電腦設定」原則具有較高的優先順序 | 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 | 啟用，15分鐘以下，但須大於0分鐘 | CCE-ID：CCE-43773-1 |
| 255 | Windows10 Computer Settings | TWGCB-01-005-0255 | Windows元件 | 設定已斷線工作階段的時間限制 | * 此項原則設定可讓使用者為已中斷連線的遠端桌面服務工作階段設定時間限制 * 如果啟用此項原則設定，經過指定的時間後會將已中斷連線的工作階段從伺服器中刪除。若要強制使用預設行為(無限期保留中斷連線的工作階段)，請選取「永不」。如果使用者有主控台工作階段，則不適用已中斷連線工作階段的時間限制 * 如果停用或未設定此項原則設定，已中斷連線的工作階段會無限期保留。使用者可以在遠端桌面工作階段主機設定工具的「工作階段」索引標籤上，指定已中斷連線工作階段的時間限制 * 注意：此項原則設定同時出現在「電腦設定」和「使用者設定」中。如果兩個原則都已設定，「電腦設定」原則具有較高的優先順序 | 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 | 啟用，1分鐘 | CCE-ID：CCE-42155-2 |
| 256 | Windows10 Computer Settings | TWGCB-01-005-0256 | Windows元件 | 結束後不刪除暫存資料夾 | * 此項原則設定決定在使用者登出時，遠端桌面服務是否會保留使用者每一工作階段的暫存資料夾 * 如果啟用此項原則設定，使用者登出工作階段時，每一工作階段的暫存資料夾會保留下來 * 如果停用此項原則設定，使用者登出時，就會刪除暫存資料夾，即使系統管理員已在遠端桌面工作階段主機設定工具中指定了不一樣的設定 * 如果未設定此項原則設定，則遠端桌面服務會在使用者登出時，刪除遠端電腦上的暫存資料夾，除非伺服器系統管理員指定了不一樣的設定 * 注意：此項設定只有在伺服器使用每一工作階段的暫存資料夾時，才會生效。也就是說，如果啟用「不要使用每一工作階段的暫存資料夾」設定，則上述設定無效 | 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\暫存資料夾\結束後不刪除暫存資料夾 | 停用 | CCE-ID：CCE-42641-1 |
| 257 | Windows10 Computer Settings | TWGCB-01-005-0257 | Windows元件 | 不要使用每一工作階段的暫存資料夾 | * 此項原則設定決定是否禁止遠端桌面服務建立特定工作階段的暫存資料夾 * 如果啟用此項原則設定，就不會建立每一工作階段的暫存資料夾。遠端電腦上所有工作階段的使用者暫存檔會儲存在遠端電腦上使用者設定檔資料夾下的共用Temp資料夾中 * 如果停用此項原則設定，即使在遠端桌面工作階段主機設定工具中指定了不一樣的設定，也一律會建立每一工作階段的暫存資料夾 * 如果未設定此項原則設定，則除非在遠端桌面工作階段主機設定工具中指定了其他設定，否則會建立每一工作階段的暫存資料夾 | 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\暫存資料夾\不要使用每一工作階段的暫存資料夾 | 停用 | CCE-ID：CCE-44111-3 |
| 258 | Windows10 Computer Settings | TWGCB-01-005-0258 | Windows元件 | 需要安全的RPC通訊 | * 此項原則設定決定伺服器與所有用戶端在遠端桌面工作階段需透過安全或非安全性的RPC通訊。可以透過此項原則設定，只允許已驗證及已加密的要求，來加強與用戶端的RPC通訊安全性 * 若啟用此項原則設定，遠端桌面服務會接受支援安全要求的RPC用戶端提出的要求，但不允許與不信任的用戶端進行非安全性通訊 * 若停用此項原則設定，遠端桌面服務一律會對所有RPC傳輸要求安全性。不過，如果RPC用戶端未回應要求，即允許非安全性通訊 * 若未設定此項原則設定，則允許非安全性通訊 * 注意：RPC介面是用於管理及設定遠端桌面服務 | 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\需要安全的RPC通訊 | 啟用 | CCE-ID：CCE-42710-4 |
| 259 | Windows10 Computer Settings | TWGCB-01-005-0259 | Windows元件 | 不要將 [關閉Windows]對話方塊中的預設選項調整為[安裝更新並關機] | * 此項原則設定允許使用者管理是否要讓「安裝更新並關機」選項成為「關閉Windows」對話方塊中的預設選擇 * 如果啟用此項原則設定，則無論「您要電腦執行什麼工作?」清單中是否有可用的「安裝更新並關機」選項，使用者上次關機時在「關閉Windows」對話方塊中所選擇的選項(休眠、重新開機等)就會是預設選項 * 如果停用或未設定此項原則設定，如果使用者在「開始」功能表中選擇「關機」選項時有可安裝的可用更新，則「關閉Windows」對話方塊中的預設選項即為「安裝更新並關機」 * 請注意，如果啟用了「電腦設定\系統管理範本\Windows元件\Windows Update\不要在[關閉Windows]對話方塊中顯示[安裝更新並關機選項]」原則設定，則此項原則設定就無效 | 電腦設定\系統管理範本\Windows元件\Windows Update\不要將 [關閉Windows]對話方塊中的預設選項調整為[安裝更新並關機] | 停用 | CCE-ID：CCE-44380-4 |
| 260 | Windows10 Computer Settings | TWGCB-01-005-0260 | Windows元件 | 不要連線到任何Windows Update網際網路位置 | * 即使Windows Update設定為從內部網路更新服務接收更新，它仍會定期從公用Windows Update服務擷取資訊，以便未來可以連線到Windows Update以及Microsoft Update或Windows市集之類的其他服務 * 啟用此項原則將停用該功能，也可能造成Windows市集這類公用服務的連線停止運作 * 注意：這部電腦設定為使用「指定近端內部網路Microsoft更新服務的位置」原則連線到內部網路更新服務時，才適用此項原則 | 電腦設定\系統管理範本\Windows元件\Windows Update\不要連線到任何Windows Update網際網路位置 | 啟用 | CCE-ID：CCE-43115-5 |
| 261 | Windows10 Computer Settings | TWGCB-01-005-0261 | Windows元件 | 不要在[關閉Windows]對話方塊中顯示[安裝更新並關機]選項 | * 此項原則設定決定是否要在「關閉Windows」對話方塊中顯示「安裝更新並關機」選項 * 如果啟用此項原則設定，即使當使用者在「開始」功能表中選擇「關機」選項且有可用的更新可以安裝，也不會在「關閉Windows」對話方塊中出現「安裝更新並關機」的選擇 * 如果停用或未設定此項原則設定，如果當使用者在「開始」功能表中選擇「關機」選項時有可用的更新，則「關閉Windows」對話方塊中就會有「安裝更新並關機」選項可供使用 | 電腦設定\系統管理範本\Windows元件\Windows Update\不要在[關閉Windows]對話方塊中顯示[安裝更新並關機]選項 | 停用 | CCE-ID：CCE-44263-2 |
| 262 | Windows10 Computer Settings | TWGCB-01-005-0262 | Windows元件 | 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 | * 此項原則設定決定有使用者登入時，是否要自動重新開機以完成排定的自動更新安裝 * 如果啟用此項原則設定，自動更新將不會在已排程安裝時如果已經有使用者登入到電腦時自動重新啟動電腦。取而代之的是，自動更新將通知使用者重新開機 * 如果停用或未設定此項原則設定，自動更新將通知使用者，電腦將在5分鐘後自動重新啟動來完成安裝 * 注意：此原則只套用在當自動更新是設定成要在排程安裝時執行更新。如果停用「設定自動更新」原則，此原則就無效 | 電腦設定\系統管理範本\Windows元件\Windows Update\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 | 停用 | CCE-ID：CCE-42867-2 |
| 263 | Windows10 Computer Settings | TWGCB-01-005-0263 | Windows元件 | 重新排程已經排程好的自動更新安裝 | * 此項原則設定決定自動更新在系統啟動之後，並要繼續上次錯過的已排程的安裝前，所要等候的時間 * 如果啟用此項原則設定，之前尚未發生的已排程安裝將在電腦下次啟動後以指定的分鐘數後開始 * 如果停用此項原則設定，錯過的排程安裝將會於下一個排程安裝同時發生 * 如果尚未設定此項原則設定，錯過的排程安裝將會於下次開機後一分鐘發生 * 注意：此原則只套用在當自動更新是設定成要在排程安裝時執行更新。如果停用「設定自動更新」原則，此原則就無效 | 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 | 啟用，1分鐘 | CCE-ID：CCE-42054-7 |
| 264 | Windows10 Computer Settings | TWGCB-01-005-0264 | Windows元件 | 設定自動更新 | * 此項原則設定決定這部電腦是否將經由Windows的自動更新服務接收安全性更新和其他重要的下載 * 如果啟用自動更新服務，必須於群組原則設定中選取以下四個選項的其中一個： * 2=通知我下載並自動安裝：當Windows找到適用於這部電腦的更新時，狀態列會出現一個帶有訊息的圖示，表示已經準備好下載更新了。按圖示或訊息，提供選項選取特定的更新。Windows然後在背景裡下載所選取的更新。下載完成後，圖示會再次出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 3=自動下載並通知我安裝：(預設設定)Windows找到要套用在電腦上的更新和，以及在背景裡下載這些更新(不通知使用者或插斷此處理)。下載完成後，圖示會出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 4=自動下載和排程安裝：使用群組原則設定的選項來指定排程。如果不指定排程的話，所有安裝的預設排程是每天早上3：00。如果有任何更新需要重新開機才能完成安裝的話，Windows將自動重新啟動電腦(如果使用者在Windows準備好重新啟動時登入電腦，使用者將收到通知，並且可以選擇延後重新啟動的時間) | 電腦設定\系統管理範本\Windows元件\Windows Update\設定自動更新 | 啟用，  3-自動下載並通知我安裝 | CCE-ID：CCE-42846-6 |
| 265 | Windows10 Computer Settings | TWGCB-01-005-0265 | Windows元件 | 允許基本驗證(用戶端) | * 此項原則設定可管理Windows遠端管理(WinRM)用戶端是否使用基本驗證 * 如果啟用此項原則設定，WinRM用戶端會使用基本驗證。如果將WinRM設定為使用HTTP傳輸，使用者名稱及密碼就會以純文字在網路上傳送 * 如果停用或未設定此項原則設定，WinRM用戶端不會使用基本驗證 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理(WinRM)\WinRM用戶端\允許基本驗證 | 停用 | CCE-ID：CCE-44257-4 |
| 266 | Windows10 Computer Settings | TWGCB-01-005-0266 | Windows元件 | 允許未加密的流量(用戶端) | * 此項原則設定可管理Windows遠端管理(WinRM)用戶端是否透過網路傳送和接收未加密的訊息 * 如果啟用此項原則設定，WinRM用戶端會透過網路傳送和接收未加密的訊息 * 如果停用或未設定此項原則設定，WinRM用戶端只會透過網路傳送或接收加密的訊息 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理(WinRM)\WinRM用戶端\允許未加密的流量 | 停用 | CCE-ID：CCE-42599-1 |
| 267 | Windows10 Computer Settings | TWGCB-01-005-0267 | Windows元件 | 不允許摘要式驗證 | * 此項原則設定可管理Windows遠端管理(WinRM)用戶端是否使用摘要式驗證 * 如果啟用此項原則設定，WinRM用戶端不會使用摘要式驗證 * 如果停用或未設定此項原則設定，WinRM用戶端會使用摘要式驗證 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理 (WinRM)\WinRM用戶端\不允許摘要式驗證 | 啟用 | CCE-ID：CCE-42295-6 |
| 268 | Windows10 Computer Settings | TWGCB-01-005-0268 | Windows元件 | 允許未加密的流量(服務) | * 此項原則設定可管理Windows遠端管理(WinRM)服務是否透過網路傳送和接收未加密的訊息 * 如果啟用此項原則設定，WinRM用戶端會透過網路傳送和接收未加密的訊息 * 如果停用或未設定此項原則設定，WinRM用戶端只會透過網路傳送或接收加密的訊息 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理(WinRM)\WinRM服務\允許未加密的流量 | 停用 | CCE-ID：CCE-44119-6 |
| 269 | Windows10 Computer Settings | TWGCB-01-005-0269 | Windows元件 | 不允許WinRM儲存RunAs認證 | * 此項原則設定可管理Windows遠端管理(WinRM)服務是否不允許儲存任何外掛程式的RunAs認證 * 如果啟用此項原則設定，WinRM服務將不允許任何外掛程式設定RunAsUser或RunAsPassword設定值。如果外掛程式已經設定RunAsUser及RunAsPassword設定值，則會從這部電腦的認證儲存區刪除RunAsPassword設定值 * 如果停用或未設定此項原則設定，WinRM服務將允許外掛程式設定RunAsUser和RunAsPassword設定值，而且可安全地儲存RunAsPassword值 * 如果啟用後又停用此項原則設定，必須重設先前設定的所有RunAsPassword值 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理 (WinRM)\WinRM服務\不允許WinRM儲存RunAs認證 | 啟用 | CCE-ID：CCE-43543-8 |
| 270 | Windows10 Computer Settings | TWGCB-01-005-0270 | Windows元件 | 設定Windows Defender SmartScreen | * 此項原則設定可開啟或關閉Windows Defender SmartScreen的行為 * Windows Defender SmartScreen會在從網際網路執行無法辨識的程式或已知有害的應用程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給Microsoft * 如果啟用此項原則設定，將會為所有使用者開啟SmartScreen。可以透過設定下列其中一個選項來控制行為： * 警告並防止略過 * 警告 * 如果使用「警告」選項啟用此原則，SmartScreen對話方塊將警告使用者應用程式看似可疑，但是將允許使用者略過該警告並繼續執行 * 如果使用者告訴SmartScreen執行應用程式，則SmartScreen不會再針對該應用程式警告使用者 * 如果停用此項原則設定，將會為所有使用者關閉SmartScreen。如果使用者嘗試執行來自網際網路的可疑應用程式，將不會收到警告 * 如果未設定此項原則，預設將會啟用SmartScreen，但使用者可變更其設定 | 電腦設定\系統管理範本\Windows元件\檔案總管\設定Windows Defender SmartScreen | 啟用：警告並防止略過 | CCE-ID：CCE-43114-8 |
| 271 | Windows10 Computer Settings | TWGCB-01-005-0271 | Windows元件 | 關閉檔案總管的資料執行防止 | 此項原則設定決定是否關閉檔案總管的資料執行防止，停用資料執行防止可使某些舊版的外掛應用程式不需終止檔案總管即可執行 | 電腦設定\系統管理範本\Windows元件\檔案總管\關閉檔案總管的資料執行防止 | 停用 | CCE-ID：CCE-44085-9 |
| 272 | Windows10 Computer Settings | TWGCB-01-005-0272 | Windows元件 | 損毀時關閉終止堆集 | 此項原則設定決定損毀時停用終止堆集可讓特定的舊版外掛應用程式不需立即中止檔案總管即可運作，雖然檔案總管稍後可能仍會無預期地終止 | 電腦設定\系統管理範本\Windows元件\檔案總管\損毀時關閉終止堆集 | 停用 | CCE-ID：CCE-42996-9 |
| 273 | Windows10 Computer Settings | TWGCB-01-005-0273 | Windows元件 | 關閉殼層通訊協定受保護模式 | * 此項原則設定決定殼層通訊協定可以擁有的功能數量 * 當使用這個通訊協定的完整功能時，應用程式可以開啟資料夾並且啟動檔案。受保護模式會降低這個通訊協定的功能，只允許應用程式開啟一組有限的資料夾。處於受保護模式時，應用程式無法以這個通訊協定開啟檔案。建議讓這個通訊協定處於受保護模式，以提高Windows的安全性 * 如果啟用此項原則設定，則會完整啟用通訊協定，允許開啟資料夾及檔案 * 如果停用此項原則設定，則通訊協定處於受保護模式，只允許應用程式開啟一組有限的資料夾 * 如果未設定此項原則設定，通訊協定將會處於受保護模式，只允許應用程式開啟一組有限的資料夾 | 電腦設定\系統管理範本\Windows元件\檔案總管\關閉殼層通訊協定受保護模式 | 停用 | CCE-ID：CCE-43569-3 |
| 274 | Windows10 Computer Settings | TWGCB-01-005-0274 | Windows元件 | 關閉遊戲資訊下載 | * 此項原則設定決定是否管理來自Windows Metadata Services之Game Box圖片及評分的下載 * 如果啟用此設定，則不會下載包含Game Box圖片及評分的遊戲資訊 * 如果停用或未設定此設定，則會從Windows Metadata Services下載遊戲資訊 | 電腦設定\系統管理範本\Windows元件\遊戲總管\關閉遊戲資訊下載 | 啟用 | 適用1803以前版本  CCE-ID：CCE-43409-2 |
| 275 | Windows10 Computer Settings | TWGCB-01-005-0275 | Windows元件 | 關閉遊戲更新 | * 此項原則設定決定是否管理從Windows Metadata Services下載遊戲更新資訊 * 如果啟用此項原則設定，將不會下載遊戲更新資訊 * 如果停用或未設定此設定，則會從Windows Metadata Services下載遊戲更新資訊 | 電腦設定\系統管理範本\Windows元件\遊戲總管\關閉遊戲更新 | 啟用 | 適用1803以前版本  CCE-ID：CCE-43083-5 |
| 276 | Windows10 Computer Settings | TWGCB-01-005-0276 | Windows元件 | 在重新開機後，自動登入並鎖定最後一個互動式使用者 | * 此項原則設定可控制裝置是否在Windows Update重新啟動系統之後自動登入最後一個互動式使用者 * 如果啟用或未設定此項原則設定，裝置會安全地儲存使用者的認證(包括使用者名稱、網域和加密的密碼)，在Windows Update重新啟動之後設定自動登入 * Windows Update重新啟動之後，使用者會自動登入，且工作階段會自動以針對該使用者設定的所有鎖定畫面的應用程式鎖定 * 如果停用此項原則設定，裝置不會儲存Windows Update重新啟動之後自動登入的使用者認證。系統重新啟動之後，使用者鎖定畫面的應用程式不會重新啟動 | 電腦設定\系統管理範本\Windows元件\Windows登入選項\在重新開機後，自動登入並鎖定最後一個互動式使用者 | 停用 | CCE-ID：CCE-42820-1 |
| 277 | Windows10 Computer Settings | TWGCB-01-005-0277 | Windows元件 | 於使用者登入期間，報告登入伺服器無法使用 | * 此項原則設定決定如果使用者在登入期間無法聯絡登入伺服器，並使用先前儲存的帳戶資訊來登入該使用者時，是否應通知使用者 * 如果啟用此項原則設定，就會在使用者使用快取的認證登入時，向使用者顯示通知快顯 * 如果停用或未設定此項原則設定，則不會向使用者顯示任何快顯 | 電腦設定\系統管理範本\Windows元件\Windows登入選項\於使用者登入期間，報告登入伺服器無法使用 | 啟用 | CCE-ID：CCE-41534-9 |
| 278 | Windows10 Computer Settings | TWGCB-01-005-0278 | Windows元件 | 允許Cortana | * 此項原則決定是否在裝置上允許使用Cortana * 若啟用或未設定此項原則設定，將在裝置上允許使用Cortana * 若為停此項原則設定，Cortana將會被關閉。當Cortana關閉時，使用者仍可使用裝置和網際網路搜尋 | 電腦設定\系統管理範本\Windows元件\搜尋\允許Cortana | 停用 | CCE-ID：CCE-42536-3 |
| 279 | Windows10 Computer Settings | TWGCB-01-005-0279 | Windows元件 | 允許加密檔案索引 | * 此項原則設定允許對加密項目編製索引 * 如果啟用此項原則設定，索引將嘗試解密，並為內容編製索引(但仍適用存取限制) * 如果停用此原則設定，搜尋服務元件(包含非Microsoft元件)預期將不會為加密的項目或加密的儲存區編製索引 * 啟用或停用此設定時，會完全重建索引 * 使用者必須為索引存放位置使用完整磁碟區加密(例如BitLocker磁碟機加密或非Microsoft解決方案)，以維護加密檔案的安全性 | 電腦設定\系統管理範本\Windows元件\搜尋\允許加密檔案索引 | 停用 | CCE-ID：CCE-44286-3 |
| 280 | Windows10 Computer Settings | TWGCB-01-005-0280 | Windows元件 | 允許搜尋和Cortana使用定位 | * 此項原則設定搜尋和Cortana是否可以提供定位感知搜尋和Cortana結果 * 若啟用此項原則設定，搜尋和Cortana可以存取位置資訊 | 電腦設定\系統管理範本\Windows元件\搜尋\允許搜尋和Cortana使用定位 | 停用 | CCE-ID：CCE-42527-2 |
| 281 | Windows10 Computer Settings | TWGCB-01-005-0281 | Windows元件 | 啟用為未快取之Exchange資料夾編製索引的功能 | * 此項原則設定決定是否啟用為未快取之Exchange資料夾編製索引的功能 * 啟用此項原則可允許在Microsoft Outlook不是以快取模式執行時，針對Microsoft Exchange伺服器上的郵件項目編製索引 * 預設的搜尋行為不會為未快取的Exchange資料夾編製索引 * 停用此項原則將會停止為未快取的Exchange資料夾編製索引。委派信箱的管理是獨立於線上信箱之外。「啟用為未快取之Exchange資料夾編製索引的功能」對委派信箱沒有作用。若要停止為線上與委派信箱編製索引，必須同時停用這兩個原則 | 電腦設定\系統管理範本\Windows元件\搜尋\啟用為未快取之Exchange資料夾編製索引的功能 | 啟用 | CCE-ID：CCE-42259-2 |
| 282 | Windows10 Computer Settings | TWGCB-01-005-0282 | Windows元件 | 防止電腦加入家用群組 | * 此項原則設定決定使用者是否可以將電腦新增到家用網路上的家用群組 * 如果啟用此項原則設定，這部電腦上的使用者無法將這部電腦新增到家用群組。此項設定不影響其他網路共用功能 * 如果停用或未設定此項原則設定，則使用者可以將這部電腦新增到家用群組。但是已加入網域的電腦上的資料不會與家用群組共用 | 電腦設定\系統管理範本\Windows元件\HomeGroup\防止電腦加入家用群組 | 啟用 | CCE-ID：CCE-41583-6 |
| 283 | Windows10 Computer Settings | TWGCB-01-005-0283 | Windows元件 | 關閉定位 | * 此項原則設定會關閉這部電腦的定位功能 * 如果啟用此項原則設定，將會關閉定位功能，而且這部電腦的所有程式都將無法使用定位功能的位置資訊 * 如果停用或未設定此項原則設定，則這部電腦的所有程式都不會被禁止使用定位功能的位置資訊 | 電腦設定\系統管理範本\Windows元件\定位和感應器\關閉定位 | 啟用 | CCE-ID：CCE-42670-0 |
| 284 | Windows10 Computer Settings | TWGCB-01-005-0284 | Windows元件 | 關閉Microsoft Store應用程式 | * 拒絕或允許存取Microsoft Store應用程式 * 如果啟用此項原則設定，將拒絕存取Microsoft Store應用程式。必須能夠存取市集才能安裝應用程式更新 * 如果停用或未設定此項原則設定，將允許存取Microsoft Store應用程式 | 電腦設定\系統管理範本\Windows元件\市集\關閉Microsoft Store應用程式 | 啟用 | CCE-ID：CCE-42144-6 |
| 285 | Windows10 Computer Settings | TWGCB-01-005-0285 | Windows元件 | 停用來自Microsoft Store的所有應用程式 | * 如果停用此項原則設定，會防止啟動來自Microsoft Store的所有應用程式(不論是預先安裝或已經下載)。應用程式將不會更新。此外，也會停用Microsoft Store * 如果啟用此項原則設定，將會重新開啟所有功能 | 電腦設定\系統管理範本\Windows元件\市集\停用來自Microsoft Store的所有應用程式 | 停用 | CCE-ID：CCE-43814-3 |
| 286 | Windows10 Computer Settings | TWGCB-01-005-0286 | Windows元件 | 允許基本驗證(服務) | * 此項原則設定可管理Windows遠端管理(WinRM)服務是否接受來自遠端用戶端的基本驗證 * 如果啟用此項原則設定，WinRM服務會接受來自遠端用戶端的基本驗證 * 如果停用或未設定此項原則設定，WinRM服務不會接受來自遠端用戶端的基本驗證 | 電腦設定\系統管理範本\Windows元件\Windows遠端管理(WinRM)\WinRM服務\允許基本驗證 | 停用 | CCE-ID：CCE-41707-1 |
| 287 | Windows10 Computer Settings | TWGCB-01-005-0287 | Windows元件 | 加入Microsoft地圖 | * 此項原則設定可加入Microsoft Active Protection Services(MAPS)，是協助使用者選擇如何回應潛在威脅的線上社群。這個社群也可協助停止散佈新惡意軟體的感染 * 可以選擇傳送偵測到之軟體的基本或其他資訊。額外的資訊可協助Microsoft建立新的安全情報，以協助它保護使用者的電腦。這項資訊可能包含移除有害軟體後，偵測到的項目在使用者電腦上的位置，系統會被自動收集和傳送此資訊。在某些情況下，可能會意外將個人資訊傳送給Microsoft。不過，Microsoft不會使用這些資訊來識別使用者的身分或與使用者聯繫 * 啟用時，此項原則設定將可能傳送給Microsoft之資訊限制為以下設定： * 已停用 * 基本MAPS * 進階MAPS * 基本MAPS將會傳送有關偵測到之軟體的基本資訊給Microsoft，包括軟體來源、使用者採取的動作或自動採取的動作，以及這些動作是否成功 * 進階MAPS除了基本資訊之外，還會將更多有關惡意軟體、間諜軟體以及潛在的垃圾軟體的資訊傳送給Microsoft，包括軟體位置、檔案名稱、軟體運作方式，以及使用者對電腦的影響 * 如果啟用此項原則設定，將以指定的成員資格加入Microsoft MAPS * 如果停用或未設定此項原則設定，使用者將不會加入Microsoft MAPS * 在Windows 10中，基本MAPS已無法使用，因此將值設定為基本MAPS或進階MAPS會將裝置註冊到進階MAPS | 電腦設定\系統管理範本\Windows元件\Windows Defender防毒軟體\MAPS\加入Microsoft地圖 | 啟用：停用 |  |
| 288 | Windows10 Computer Settings | TWGCB-01-005-0288 | Windows元件 | 防止Windows Media DRM網路網路存取 | * 此項原則設定決定是否防止Windows Media Digital Rights Management(DRM)存取網際網路(或內部網路) * 如果啟用此項原則設定，Windows Media DRM將無法存取網際網路(或內部網路)以取得授權及進行安全性升級 * 如果停用或尚未設定此項原則設定時，Windows Media DRM會正常運作，並且會連線到網際網路(或內部網路)以取得授權、下載安全性升級及執行授權還原 | 電腦設定\系統管理範本\Windows元件\Windows Media Digital Rights Management\防止Windows Media DRM網路網路存取 | 啟用 | CCE-ID：CCE-41506-7 |
| 289 | Windows10 Computer Settings | TWGCB-01-005-0289 | Windows元件 | 停用遠端桌面共用 | * 此項原則設定決定是否禁止使用NetMeeting的遠端桌面共用功能 * 如果啟用此項原則設定，使用者將無法自遠端進行設定，或者使用這項功能自遠端控制他們的電腦 | 電腦設定\系統管理範本\Windows元件\NetMeeting\停用遠端桌面共用 | 啟用 | CCE-ID：CCE-42230-3 |
| 290 | Windows10 Computer Settings | TWGCB-01-005-0290 | Windows元件 | 防止下載隨函附件 | * 此項原則設定可防止使用者從摘要下載隨函附件(檔案附件)到使用者的電腦 * 如果啟用此項原則設定，使用者將無法透過「摘要」內容頁將Feed Sync Engine設成下載隨函附件。開發人員無法透過「摘要」API來變更下載設定 * 如果停用或未設定此項原則設定，使用者可以透過「摘要」內容頁來設定Feed Sync Engine下載隨函附件。開發人員可以透過「摘要API」來變更下載設定 | 電腦設定\系統管理範本\Windows元件\RSS摘要\防止下載隨函附件 | 啟用 | CCE-ID：CCE-42215-4 |
| 291 | Windows10 Computer Settings | TWGCB-01-005-0291 | Windows元件 | 不允許執行數位購物服務區 | * 此項原則設定決定是否可執行數位購物服務區 * 「數位購物服務區」是與Windows Marketplace關聯的專屬下載管理員，也是一種Windows功能，它可以用來管理和下載使用者所需的產品並儲存在使用者的「Windows Marketplace數位購物服務區」 * 如果啟用此項原則設定，「數位購物服務區」將不會執行 * 如果停用或未設定此項原則設定，則「數位購物服務區」就可以執行 | 電腦設定\系統管理範本\Windows元件\數位購物服務區\不允許執行數位購物服務區 | 啟用 | CCE-ID：CCE-41912-7 |
| 292 | Windows10 Computer Settings | TWGCB-01-005-0292 | Windows元件 | 關閉清查收集器 | * 此項原則設定可以控制清查收集器的狀態 * 清查收集器會清查系統中的應用程式、檔案、裝置和驅動程式，並將資訊傳送給Microsoft。這項資訊可用來協助診斷相容性問題 * 如果啟用此項原則設定，則會關閉清查收集器，而且不會傳送資料給Microsoft。同時也會停用透過程式相容性助理收集安裝資料的功能 * 如果停用或未設定此項原則設定，則會開啟清查收集器 * 注意：如果關閉客戶經驗改進計畫，此項原則設定將不會發生任何作用。清查收集器將會被關閉 | 電腦設定\系統管理範本\Windows元件\應用程式相容性\關閉清查收集器 | 啟用 | CCE-ID：CCE-44397-8 |
| 293 | Windows10 Computer Settings | TWGCB-01-005-0293 | Windows元件 | 關閉Microsoft消費者體驗 | * 若啟用此項原則設定，使用者將再也不會看到Microsoft所提供的個人化建議與有關其Microsoft帳戶的通知 * 若停用或未設定此項原則設定，使用者可以看到Microsoft 所提供的建議與有關其Microsoft帳戶的通知 * 注意：此設定只適用於Windows10企業版與教育版SKU | 電腦設定\系統管理範本\Windows元件\雲端內容\關閉Microsoft消費者體驗 | 啟用 | CCE-ID：CCE-42547-0 |
| 294 | Windows10 Computer Settings | TWGCB-01-005-0294 | Windows元件 | 防止使用OneDrive儲存檔案 | * 此項原則設定可防止應用程式和功能使用OneDrive上的檔案 * 若啟用此項原則設定： * 使用者不能從OneDrive應用程式和檔案選擇器存取 OneDrive * Windows市集應用程式不能使用WinRT API存取OneDrive * OneDrive不會顯示在檔案總管的瀏覽窗格中 * OneDrive檔案不會與雲端保持同步 * 使用者不能從「手機相簿」資料夾自動上傳相片和影片 * 若停用或未設定此項原則設定，應用程式和功能就可以使用OneDrive檔案儲存空間 | 電腦設定\系統管理範本\Windows元件\OneDrive\防止使用OneDrive儲存檔案 | 啟用 | CCE-ID：CCE-44160-0 |
| 295 | Windows10 Computer Settings | TWGCB-01-005-0295 | Windows元件 | 使用增強式反詐騙 | * 此項原則設定決定是否為Windows Hello臉部驗證使用增強式反詐騙功能 * 若啟用此項原則設定，Windows將要求設備上的所有使用者為Windows Hello臉部驗證使用增強式反詐騙功能。這會在不支援增強式反詐騙的裝置上停用Windows Hello臉部驗證 * 若停用或未設定此項原則設定， Windows不會要求為Windows Hello臉部驗證使用增強式反詐騙功能 | 電腦設定\系統管理範本\Windows元件\生物識別技術\臉部功能\使用增強式反詐騙 | 啟用 | CCE-ID：CCE-44433-1 |
| 296 | Windows10 Computer Settings | TWGCB-01-005-0296 | Windows元件 | 允許Windows應用程式在使用者間共用應用程式資料 | * 此項原則設定管理Windows應用程式在多個安裝該應用程式之使用者間共用資料的功能 * 若啟用此項原則設定，Windows應用程式將可以與應用程式的其他執行個體共用應用程式資料。資料會透過SharedLocal資料夾共用。這個資料夾可透過Windows.Storage API來存取 * 若停用此項原則設定，Windows應用程式將無法與該應用程式的其他執行個體共用應用程式資料。如果預先停用此原則，任何預先共用的應用程式資料將保留於SharedLocal資料夾中 | 電腦設定\系統管理範本\Windows元件\應用程式套件部署\允許Windows應用程式在使用者間共用應用程式資料 | 停用 | CCE-ID：CCE-42502-5 |
| 297 | Windows10 Computer Settings | TWGCB-01-005-0297 | Windows元件 | 允許遠端殼層存取 | * 此項原則設定可決定遠端殼層的存取權 * 若啟用或未設定此項原則設定，伺服器會接受新的遠端殼層連線 * 若停用此項原則設定，則伺服器會拒絕新的遠端殼層連線 | 電腦設定\系統管理範本\Windows元件\Windows遠端殼層\允許遠端殼層存取 | 停用 | CCE-ID：CCE-44312-7 |
| 298 | Windows10 Computer Settings | TWGCB-01-005-0298 | 系統\緩和選項 | 封鎖未受信任的字型 | * 此項原則設定決定是否防止程式載入未受信任的字型 * 未受信任的字型為安裝於%Windir%\Fonts目錄外之任何字型。此功能有3種選項： * 封鎖未受信任的字型並記錄事件 * 不封鎖未受信任的字型 * 記錄事件，而不封鎖未受信任的字型 * 如果還沒準備好在機關中部署這項功能，可以使用「記錄事件，而不封鎖未受信任的字型」模式查看封鎖未受信任的字型是否會產生任何相容性之問題 | 電腦設定\系統管理範本\系統\緩和選項\封鎖未受信任的字型 | 啟用，封鎖未受信任的字型並紀錄 | CCE-ID：CCE-43801-0 |
| 299 | Windows10 Computer Settings | TWGCB-01-005-0299 | 系統\Kerberos | 支援使用憑證進行裝置驗證 | * 要支援裝置使用憑證驗證，裝置帳戶網域需要支援使用憑證進行電腦帳戶驗證，並需要可連線至網域控制站(DC)的能力 * 此項原則設定可讓使用者設定Kerberos支援嘗試使用裝置的憑證驗證到網域 * 若啟用此項原則設定，裝置憑證將根據下列選項選取： * 自動：裝置將嘗試使用本身的憑證驗證。如果網域控制站(DC)不支援使用憑證進行電腦帳戶驗證，則會嘗試使用密碼驗證 * 強制：裝置將總是使用本身的憑證驗證。如果找不到支援使用憑證進行電腦帳戶驗證的網域控制站(DC)，則驗證會失敗 * 若未設定此項原則設定，可使用「自動」 | 電腦設定\系統管理範本\系統\Kerberos\支援使用憑證進行裝置驗證 | 啟用-自動 | CCE-ID：CCE-42501-7 |
| 300 | Windows10 Computer Settings | TWGCB-01-005-0300 | 印表機 | 擴充指向並列印連線以搜尋Windows Update | * 此項原則設定決定可讓使用者管理用戶端電腦在何處搜尋指向並列印驅動程式 * 如果啟用此項原則設定，用戶端電腦在本機驅動程式存放區與伺服器驅動程式快取中找不到相容驅動程式後，會繼續從Windows Update搜尋相容的指向並列印驅動程式 * 如果停用此項原則設定，用戶端電腦只會在本機驅動程式存放區和伺服器驅動程式快取中搜尋相容的指向並列印驅動程式。如果找不到相容驅動程式，則指向並列印連線會失敗 * 如果未設定此項原則設定，其行為須視所使用的Windows版本而定。根據預設，Windows旗艦版、專業版及家用SKU版會視需求從Windows Update搜尋相容的指向並列印驅動程式。然而，如果使用其他Windows版本，如Windows企業版、所有的Windows Server 2008 R2及更新版本，就必須明確啟用此項原則設定才會有相同的行為 | 電腦設定\系統管理範本\印表機\擴充指向並列印連線以搜尋Windows Update | 停用 | CCE-ID：CCE-41484-7 |
| 301 | Windows10 User Settings | TWGCB-01-005-0301 | 附件管理員 | 不要保留檔案附件的區域資訊 | * 此項原則設定決定使用者管理Windows時，是否用資訊的來源區域來標示附件檔案(例如：受限、網際網路、內部網路、本機)。這必須要透過NTFS才能正確運作，在FAT32上則會在不另通知的情況下失敗。如果沒有保留區域資訊，Windows無法正確評定風險 * 如果啟用此項原則設定，Windows就不會標示附件檔案的區域資訊 * 如果停用或未設定此項原則設定，Windows就會標示附件檔案的區域資訊 | 使用者設定\系統管理範本\Windows元件\附件管理員\不要保留檔案附件的區域資訊 | 停用 | CCE-ID：CCE-42262-6 |
| 302 | Windows10 User Settings | TWGCB-01-005-0302 | 附件管理員 | 隱藏移除區域資訊的機制 | * 此項原則設定決定使用者是否可透過按一下檔案內容頁上的「解除封鎖」按鈕，或使用安全警告對話方塊裡的核取方塊，來手動移除已儲存附件檔案的區域資訊。移除區域資訊可讓使用者開啟Windows禁止使用者開啟的具有潛在危險之附件檔案 * 如果啟用此項原則設定，Windows會隱藏核取方塊以及「解除封鎖」按鈕 * 如果停用或未設定此項原則設定，Windows會顯示核取方塊以及「解除封鎖」按鈕 | 使用者設定\系統管理範本\Windows元件\附件管理員\隱藏移除區域資訊的機制 | 啟用 | CCE-ID：CCE-43839-0 |
| 303 | Windows10 User Settings | TWGCB-01-005-0303 | 附件管理員 | 開啟附件時通知防毒程式 | * 此項原則設定可讓使用者管理已登錄防毒程式的通知行為。如果已登錄多種程式，將會全部通知。如果已登錄的防毒程式已經執行即時檢查或即時掃描傳送到電腦的電子郵件伺服器上之所有檔案，任何其他呼叫將會是多餘的 * 如果啟用這項原則，Windows會命令已登錄的防毒程式在使用者開啟附件檔案時掃描該檔案。如果防毒程式失敗，將無法開啟附件 * 如果停用這項原則，Windows就不會在開啟附件檔案時呼叫已登錄防毒程式 * 如果沒有設定這項原則，Windows就不會在開啟附件檔案時呼叫已登錄防毒程式 | 使用者設定\系統管理範本\Windows元件\附件管理員\開啟附件時通知防毒程式 | 啟用 | CCE-ID：CCE-43545-3 |
| 304 | Windows10 User Settings | TWGCB-01-005-0304 | 網路共用 | 防止使用者共用其設定檔內的檔案 | * 此項原則設定會指定使用者是否可以共用設定檔內的檔案。根據預設，系統管理員在電腦中加以選擇之後，便允許使用者與其網路上的其他使用者共用他們設定檔內的檔案。系統管理員可以使用共用精靈，在電腦上進行選擇，以共用使用者設定檔內的檔案 * 如果啟用此項原則設定，使用者將不能使用共用精靈，來共用其設定檔內的檔案。同時，共用精靈也不會在%root %users上建立共用，而且該精靈只可用來在資料夾上建立SMB共用 * 如果停用或未設定此項原則設定，系統管理員在電腦中加以選擇之後，使用者便可共用其使用者設定檔中的檔案 | 使用者設定\系統管理範本\Windows元件\網路共用\防止使用者共用其設定檔內的檔案 | 啟用 | CCE-ID：CCE-43095-9 |
| 305 | Windows10 User Settings | TWGCB-01-005-0305 | 網際網路通訊設定 | 關閉說明分級 | * 此項原則設定決定使用者是否可以提供說明內容分級 * 若啟用此項原則設定，則會禁止在說明內容中加入分級控制 * 若停用或未設定此項原則設定，說明主題中則會加入分級控制。使用者可以使用分級控制提供「說明及支援」內容的品質及實用性的意見回饋 | 使用者設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉說明分級 | 啟用 | CCE-ID：CCE-41603-2 |
| 306 | Windows10 User Settings | TWGCB-01-005-0306 | 個人化 | 啟用螢幕保護裝置 | * 此項原則設定決定是否啟用桌面螢幕保護裝置 * 如果啟用此項原則設定，只要下列兩項條件成立，螢幕保護裝置就會執行： * 已透過「螢幕保護裝置執行檔名稱」設定或用戶端電腦上的「控制台」，在用戶端上指定有效的螢幕保護裝置 * 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 * 如果停用此項原則設定，螢幕保護裝置不會執行。此外，此項設定會停用「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊中的「螢幕保護裝置」區段。因此，使用者無法變更螢幕保護裝置選項 * 如果未設定此項原則設定，此項設定對系統沒有作用 | 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 | 啟用 | CCE-ID：CCE-42836-7 |
| 307 | Windows10 User Settings | TWGCB-01-005-0307 | 個人化 | 以密碼保護螢幕保護裝置 | * 此項原則設定決定是否要以密碼保護電腦上使用的螢幕保護裝置 * 如果啟用此項原則設定，所有螢幕保護裝置都會受到密碼保護 * 如果停用此項原則設定，則無法在任何螢幕保護裝置上設定密碼保護。此設定也會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的「受密碼保護」核取方塊，以防止使用者變更密碼保護設定 * 如果未設定此項原則設定，使用者可以選擇是否要在每個螢幕保護裝置上設定密碼保護 * 若要確保電腦受到密碼保護，必須啟用「啟用螢幕保護裝置」設定，並透過「螢幕保護裝置逾時」設定指定逾時 * 注意：若要移除「螢幕保護裝置」對話方塊，請使用「防止變更螢幕保護裝置」設定 | 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 | 啟用 | CCE-ID：CCE-43863-0 |
| 308 | Windows10 User Settings | TWGCB-01-005-0308 | 個人化 | 螢幕保護裝置逾時 | * 此項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動 * 如果已設定，這個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。如果設為零，螢幕保護裝置將不會啟動 * 在下列任一狀況下，此項設定沒有作用： * 設定已停用或未設定 * 等候時間設為零 * 「啟用螢幕保護裝置」設定已停用 * 「螢幕保護裝置執行檔名稱」設定和用戶端電腦的「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊都沒有在用戶端上指定有效的現有螢幕保護裝置程式 * 如果未設定，則會使用透過「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊在用戶端上設定的等候時間。預設值是15分鐘 | 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 | 啟用，900秒以下，但須大於0秒 | CCE-ID：CCE-43159-3 |
| 309 | Windows10 User Settings | TWGCB-01-005-0309 | 個人化 | 強制特定的螢幕保護裝置 | * 如果啟用此項原則設定，系統會在使用者的桌面上顯示指定的螢幕保護裝置。此外，此項原則設定會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的螢幕保護裝置下拉式清單，以防止使用者變更螢幕保護裝置 * 如果停用或未設定此項原則設定，則使用者可以選取任一螢幕保護裝置 * 如果啟用此項原則設定，請輸入含有螢幕保護裝置的檔案名稱(包括.scr副檔名)。如果螢幕保護裝置檔案不在%Systemroot%\System32目錄中，請輸入檔案的完整路徑 * 如果指定的螢幕保護裝置未安裝在套用此設定的電腦上，就會略過此項設定 * 注意：此項原則設定可能已被「啟用螢幕保護裝置」設定所取代。如果「啟用螢幕保護裝置」設定已停用，就會略過此項設定，而且螢幕保護裝置不會執行 | 使用者設定\系統管理範本\控制台\個人化\強制特定的螢幕保護裝置 | 啟用 | CCE-ID：CCE-42564-5 |
| 310 | Windows10 User Settings | TWGCB-01-005-0310 | 個人化 | 防止變更螢幕保護裝置 | * 防止在「個人化」或「顯示」控制台中開啟「螢幕保護裝置」對話方塊 * 此項設定會防止使用者利用「控制台」新增、設定或變更電腦上的螢幕保護裝置。但此項原則設定不會防止螢幕保護裝置執行 | 使用者設定\系統管理範本\控制台\個人化\防止變更螢幕保護裝置 | 啟用 | CCE-ID：CCE-43729-3 |
| 311 | Windows10 User Settings | TWGCB-01-005-0311 | 其他 | 在鎖定畫面上關閉快顯通知 | * 此項原則設定可在鎖定畫面上關閉快顯通知 * 如果啟用此項原則設定，應用程式將無法在鎖定畫面上引發快顯通知 * 如果停用或未設定此項原則設定，則可在鎖定畫面上啟用快顯通知，並可讓系統管理員或使用者關閉通知。此項原則設定不需重新開機或重新啟動服務就會生效 | 使用者設定\系統管理範本\[開始]功能表與工作列\通知\在鎖定畫面上關閉快顯通知 | 啟用 | CCE-ID：CCE-43847-3 |
| 312 | Windows10 User Settings | TWGCB-01-005-0312 | Windows元件 | 防止轉碼器下載 | * 此項原則設定可防止Windows Media Player下載轉碼器 * 如果啟用此項原則設定，會防止Player自動將轉碼器下載至使用者的電腦。此外，Player中「播放程式」索引標籤上的「自動下載轉碼器」核取方塊也無法使用 * 如果停用此項原則設定，轉碼器會自動下載，且無法使用「自動下載轉碼器」核取方塊 * 如果未設定此項原則設定，使用者可以變更「自動下載轉碼器」核取方塊的設定 | 使用者設定\系統管理範本\Windows元件\Windows Media Player\播放\防止轉碼器下載 | 啟用 | CCE-ID：CCE-44273-1 |
| 313 | Windows10 Firewall Settings | TWGCB-01-005-0313 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：顯示通知 | * 此項原則設定決定當程式要求Windows Defender防火牆將程式新增到程式例外清單時，是否禁止Windows Defender防火牆對使用者顯示通知 * 如果此項原則設定為「否」，Windows Defender防火牆將禁止顯示這些通知 * 如果此項原則設定為「是」，Windows Defender防火牆就會允許顯示這些通知。在「控制台」的「Windows Defender防火牆」元件中，「當Windows Defender防火牆封鎖新的程式時請通知我」核取方塊將設定為選取狀態，且系統管理員無法將其清除 * 如果未設定此項原則設定，Windows Defender防火牆會當作已停用此項原則設定，在「控制台」的「Windows Defender防火牆」元件中，「當Windows Defender防火牆封鎖新的程式時請通知我」核取方塊仍預設為選取狀態，但系統管理員可進行變更 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\顯示通知 | 是 | CCE-ID：CCE-44177-4 |
| 314 | Windows10 Firewall Settings | TWGCB-01-005-0314 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：允許單點傳播回應 | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\允許單點傳播回應 | 否 | CCE-ID：CCE-41651-1 |
| 315 | Windows10 Firewall Settings | TWGCB-01-005-0315 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\套用本機防火牆規則 | 否 | CCE-ID：CCE-42631-2 |
| 316 | Windows10 Firewall Settings | TWGCB-01-005-0316 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\套用本機連線安全性規則 | 否 | CCE-ID：CCE-41646-1 |
| 317 | Windows10 Firewall Settings | TWGCB-01-005-0317 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\輸出連線 | 允許(預設) | CCE-ID：CCE-43027-2 |
| 318 | Windows10 Firewall Settings | TWGCB-01-005-0318 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\輸入連線 | 封鎖(預設) | CCE-ID：CCE-42100-8 |
| 319 | Windows10 Firewall Settings | TWGCB-01-005-0319 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\記錄丟棄的封包 | 是 | CCE-ID：CCE-41581-0 |
| 320 | Windows10 Firewall Settings | TWGCB-01-005-0320 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\記錄成功的連線 | 是 | CCE-ID：CCE-41680-0 |
| 321 | Windows10 Firewall Settings | TWGCB-01-005-0321 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\大小限制 | 16,384 KB以上 | CCE-ID：CCE-44150-1 |
| 322 | Windows10 Firewall Settings | TWGCB-01-005-0322 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\名稱 | %windir%\system32\logfiles\firewall\domainfirewall.log | CCE-ID：CCE-42826-8 |
| 323 | Windows10 Firewall Settings | TWGCB-01-005-0323 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\防火牆狀態 | 開啟(建議選項) | CCE-ID：CCE-43236-9 |
| 324 | Windows10 Firewall Settings | TWGCB-01-005-0324 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：顯示通知 | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\顯示通知 | 是 | CCE-ID：CCE-41527-3 |
| 325 | Windows10 Firewall Settings | TWGCB-01-005-0325 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：允許單點傳播回應 | * 此項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\允許單點傳播回應 | 否 | CCE-ID：CCE-42987-8 |
| 326 | Windows10 Firewall Settings | TWGCB-01-005-0326 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\套用本機防火牆規則 | 否 | CCE-ID：CCE-41529-9 |
| 327 | Windows10 Firewall Settings | TWGCB-01-005-0327 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\套用本機連線安全性規則 | 否 | CCE-ID：CCE-43144-5 |
| 328 | Windows10 Firewall Settings | TWGCB-01-005-0328 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\防火牆狀態 | 開啟(建議選項) | CCE-ID：CCE-42914-2 |
| 329 | Windows10 Firewall Settings | TWGCB-01-005-0329 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\輸出連線 | 允許(預設) | CCE-ID：CCE-41729-5 |
| 330 | Windows10 Firewall Settings | TWGCB-01-005-0330 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\輸入連線 | 封鎖(預設) | CCE-ID：CCE-43018-1 |
| 331 | Windows10 Firewall Settings | TWGCB-01-005-0331 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\名稱 | %windir%\System32\LogFiles\Firewall\privatefirewall.log | CCE-ID：CCE-44018-0 |
| 332 | Windows10 Firewall Settings | TWGCB-01-005-0332 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\大小限制 | 16,384 KB以上 | CCE-ID：CCE-42398-8 |
| 333 | Windows10 Firewall Settings | TWGCB-01-005-0333 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\記錄丟棄的封包 | 是 | CCE-ID：CCE-42048-9 |
| 334 | Windows10 Firewall Settings | TWGCB-01-005-0334 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\記錄成功的連線 | 是 | CCE-ID：CCE-44230-1 |
| 335 | Windows10 Firewall Settings | TWGCB-01-005-0335 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：顯示通知 | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\顯示通知 | 是 | CCE-ID：CCE-42344-2 |
| 336 | Windows10 Firewall Settings | TWGCB-01-005-0336 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：允許單點傳播回應 | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\允許單點傳播回應 | 否 | CCE-ID：CCE-42562-9 |
| 337 | Windows10 Firewall Settings | TWGCB-01-005-0337 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\套用本機防火牆規則 | 否 | CCE-ID：CCE-41654-5 |
| 338 | Windows10 Firewall Settings | TWGCB-01-005-0338 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\套用本機連線安全性規則 | 否 | CCE-ID：CCE-42436-6 |
| 339 | Windows10 Firewall Settings | TWGCB-01-005-0339 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\防火牆狀態 | 開啟(建議選項) | CCE-ID：CCE-42837-5 |
| 340 | Windows10 Firewall Settings | TWGCB-01-005-0340 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\輸出連線 | 允許(預設) | CCE-ID：CCE-43407-6 |
| 341 | Windows10 Firewall Settings | TWGCB-01-005-0341 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\輸入連線 | 封鎖(預設) | CCE-ID：CCE-41611-5 |
| 342 | Windows10 Firewall Settings | TWGCB-01-005-0342 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\大小限制 | 16,384 KB以上 | CCE-ID：CCE-41585-1 |
| 343 | Windows10 Firewall Settings | TWGCB-01-005-0343 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\記錄丟棄的封包 | 是 | CCE-ID：CCE-42971-2 |
| 344 | Windows10 Firewall Settings | TWGCB-01-005-0344 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\記錄成功的連線 | 是 | CCE-ID：CCE-43884-6 |
| 345 | Windows10 Firewall Settings | TWGCB-01-005-0345 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\名稱 | %windir%\system32\logfiles\firewall\publicfirewall.log | CCE-ID：CCE-43659-2 |
| 346 | Windows10 Computer Settings | TWGCB-01-005-0346 | 進階稽核原則設定 | 稽核詳細的檔案共用 | * 此項原則設定可稽核存取共用資料夾中之檔案及資料夾的嘗試，記錄每次存取檔案或資料夾的事件，包括關於權限或用來授與或拒絕存取之其他條件的詳細資訊 * 如果設定此項原則設定，當嘗試存取共用上的檔案或資料夾時，就會產生稽核事件。系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 * 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用此項原則設定，則會稽核系統上所有共用檔案與資料夾的存取 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核詳細的檔案共用 | 失敗 |  |
| 347 | Windows10 Computer Settings | TWGCB-01-005-0347 | 進階稽核原則設定 | 稽核檔案共用 | * 此項原則設定可稽核存取共用資料夾的嘗試 * 如果設定此項原則設定，則會在嘗試存取共用資料夾時產生稽核事件。系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 * 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用此項原則設定，則會稽核系統上所有共用資料夾的存取 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核檔案共用 | 成功與失敗 |  |
| 348 | Windows10 Computer Settings | TWGCB-01-005-0348 | 進階稽核原則設定 | 稽核其他物件存取事件 | * 此項原則設定可稽核因管理工作排程器物件或COM+物件而產生之事件 * 如果是排程器工作，則會稽核下列項目： * 建立工作 * 刪除工作 * 啟用工作 * 停用工作 * 更新工作 * 如果是COM+物件，則會稽核下列項目： * 新增類別目錄物件 * 更新類別目錄物件 * 刪除類別目錄物件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核其他物件存取事件 | 成功與失敗 |  |
| 349 | Windows10 Computer Settings | TWGCB-01-005-0349 | 進階稽核原則設定 | 稽核授權原則變更 | * 此項原則設定稽核因授權原則變更而產生之事件，例如： * 指派未透過「驗證原則變更」子類別稽核的使用者權限(如SeCreateTokenPrivilege) * 移除未透過「驗證原則變更」子類別稽核的使用者權限(如SeCreateTokenPrivilege) * 加密檔案系統(EFS)原則的變更 * 物件之資源屬性的變更 * 套用至物件之集中存取原則(CAP)的變更 * 如果設定此項原則設定，則會在嘗試變更授權原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更授權原則時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核授權原則變更 | 成功 |  |
| 350 | Windows10 Computer Settings | TWGCB-01-005-0350 | 進階稽核原則設定 | MPSSVC規則層級原則變更 | * 此項原則設定可稽核因Microsoft保護服務(MPSSVC)使用之原則規則變更而產生之事件。這個服務是供Windows防火牆使用。包含下列事件： * 報告Windows防火牆服務啟動時的使用中原則 * Windows防火牆規則的變更 * Windows防火牆例外清單的變更 * Windows防火牆設定的變更 * Windows防火牆服務忽略或未套用的規則 * Windows防火牆群組原則設定的變更 * 如果設定此項原則設定，則會在嘗試變更 MPSSVC所使用的原則規則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，在MPSSVC使用的原則規則變更時則不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\MPSSVC規則層級原則變更 | 成功與失敗 |  |
| 351 | Windows10 Computer Settings | TWGCB-01-005-0351 | 進階稽核原則設定 | 稽核其他原則變更事件 | * 此項原則設定可稽核原則變更類別未稽核之其他安全性原則變更所產生的稽核事件，例如： * 信賴平台模組(TPM)設定變更 * 核心模式密碼編譯自我測試 * 密碼編譯提供者操作 * 密碼編譯內容操作或修改 * 已套用的集中存取原則(CAP)變更 * 開機設定資料(BCD)修改 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核其他原則變更事件 | 失敗 |  |
| 352 | Windows10 Computer Settings | TWGCB-01-005-0352 | 進階稽核原則設定 | 稽核PNP活動 | * 此項原則設定可在隨插即用偵測到外接式裝置時執行稽核 * 若設定此項原則設定，每當隨插即用偵測到外接式裝置時會產生稽核事件。此類別只會記錄成功稽核 * 若未設定此項原則設定，當隨插即用偵測到外接式裝置時不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核PNP活動 | 成功 |  |
| 353 | Windows10 Computer Settings | TWGCB-01-005-0353 | 進階稽核原則設定 | 稽核群組成員資格 | * 此項原則可稽核使用者登入權杖中的群組成員資格資訊。這個子類別中的事件會在建立登入工作階段的電腦上產生。對於互動式登入，安全性稽核事件會在使用者登入的電腦上產生。對於網路登入(例如存取網路上的共用資料夾)，安全性稽核事件會在主控資源的電腦上產生 * 設定此設定後，會針對每個成功的登入產生一或多個安全性稽核事件，且必須啟用「進階稽核原則設定\系統稽核原則\登入/登出」底下的「稽核登入」設定。如果單一安全性稽核事件無法容納群組成員資格資訊，則會產生多個事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核群組成員資格 | 成功 |  |
| 354 | Windows10 Computer Settings | TWGCB-01-005-0354 | 進階稽核原則設定 | 稽核其他登入/登出事件 | * 此項原則設定可稽核「登入/登出」原則設定未涵蓋之其他登入/登出相關事件，例如： * 終端機服務工作階段中斷連線 * 新的終端機服務工作階段 * 鎖定及解除鎖定工作站 * 呼叫螢幕保護裝置 * 解除螢幕保護裝置 * 偵測Kerberos重新執行攻擊，在這類攻擊中，會接收到具有相同資訊的Kerberos要求2次。這個狀況可能是網路設定錯誤而造成 * 將無線網路存取權限授與使用者或電腦帳戶 * 將有線802.1x網路存取權限授與使用者或電腦帳戶 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核其他登入/登出事件 | 成功與失敗 |  |
| 355 | Windows10 Computer Settings | TWGCB-01-005-0355 | 控制台 | 允許線上提示 | * 此項原則設定可啟用或停用擷取「設定」應用程式的線上提示與說明 * 若停用此項原則設定，「設定」將不會連絡Microsoft內容服務來擷取提示與說明內容 | 電腦設定\系統管理範本\控制台\允許線上提示 | 停用 |  |
| 356 | Windows10 Computer Settings | TWGCB-01-005-0356 | MS Security Guide | Configure SMB v1 client driver | * 停用用戶端SMBv1協定，請選擇「啟用」，並於Configure MrxSmb10 driver下拉選項中，選擇「Disable driver(recommended)」 * 警告：任何狀況下請不要選擇停用選項 * 要復原預設用戶端的SMBv1設定，請選擇請選擇「啟用」，並於Configure MrxSmb10 driver中選擇正確的預設值 * 針對Windows 8.1、Windows Server 2012R2及更高版本請選擇「自動啟動」 * 此設定所做的更改需要重新啟動才能生效 | 電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 client driver | 啟用，Configure MrxSmb10 driver：Disable driver(recommended) |  |
| 357 | Windows10 Computer Settings | TWGCB-01-005-0357 | MS Security Guide | Configure SMB v1 server | * 停用此設定將停用伺服器端SMBv1協定的處理(推薦) * 啟用此設定將啟用伺服器端SMBv1協定的處理(預設) * 此設定所做的更改需要重新啟動才能生效 | 電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 server | 停用 |  |
| 358 | Windows10 Computer Settings | TWGCB-01-005-0358 | MS Security Guide | Enable Structured Exception Handling Overwrite Protection (SEHOP) | * 如果啟用此原則，則將強制執行SEHOP * 如果停用或未設定此原則，則對於32位元處理器將不強制執行SEHOP | 電腦設定\系統管理範本\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP) | 啟用 |  |
| 359 | Windows10 Computer Settings | TWGCB-01-005-0359 | MS Security Guide | NetBT NodeType configuration | * NetBT NodeType設定決定NetBT用於註冊與解析名稱的方法： * B節點電腦使用廣播 * P節點電腦僅使用對名稱伺服器(WINS)的點對點名稱查詢 * M節點電腦先廣播，然後查詢名稱伺服器 * H節點電腦先查詢名稱伺服器，然後廣播 * 遵循以下方法通過LMHOSTS或DNS進行解析。如果存在NodeType值，它將覆蓋任何DhcpNodeType值 * 如果沒有NodeType與DhcpNodeType，也沒有WINS伺服器，電腦使用B節點，如果至少設定了WINS伺服器，則電腦使用H節點 | 電腦設定\系統管理範本\MS Security Guide\NetBT NodeType configuration | 啟用，Configure NetBT NodeType：P節點(推薦) |  |
| 360 | Windows10 Computer Settings | TWGCB-01-005-0360 | 網路\DNS用戶端 | 關閉多點傳送名稱解析 | * 此項原則設定可啟用或停用連結本機多點傳送名稱解析(LLMNR) * LLMNR是次要名稱解析通訊協定。使用LLMNR，查詢會透過單一子網路的本機網路連結，使用多點傳送從一部用戶端電腦傳送到相同子網路上同時啟用LLMNR的另一部用戶端電腦，LLMNR不需要DNS伺服器或DNS用戶端設定，可針對無法透過傳統 DNS名稱解析的狀況提供名稱解析 * 如果啟用此項原則設定，會停用用戶端電腦上所有可用的網路介面卡之LLMNR * 如果停用或未設定此項原則設定，會啟用所有可用的網路介面卡之LLMNR | 電腦設定\系統管理範本\網路\DNS用戶端\關閉多點傳送名稱解析 | 啟用 |  |
| 361 | Windows10 Computer Settings | TWGCB-01-005-0361 | 系統\認證委派 | 加密預示修復 | * 此項原則設定適用於使用CredSSP元件之應用程式(例如遠端桌面連線) * CredSSP通訊協定的某些版本有弱點，容易受到針對用戶端的加密Oracle攻擊所威脅。此項原則會控制易受攻擊的用戶端與伺服器的相容性，可設定加密預示弱點所需的保護層級 * 如果啟用此項原則設定，就會依據下列選項來選取CredSSP版本支援： * 強制使用更新的用戶端：使用CredSSP的用戶端應用程式將無法回復成不安全的版本，並且使用CredSSP的服務將不會接受未修補的用戶端。注意：除非所有遠端主機都已支援最新的版本，否則不應該部署此項設定 * 已降低影響：使用CredSSP的用戶端應用程式將無法回復成不安全的版本，但使用CredSSP的服務可接受未修補的用戶端 * 易受攻擊：使用CredSSP的用戶端應用程式可支援回復成不安全的版本，且使用CredSSP的服務可接受未修補的用戶端，進而導致遠端伺服器容易遭受攻擊 | 電腦設定\系統管理範本\系統\認證委派\加密預示修復 | 啟用，保護層級：強制使用更新的用戶端 |  |
| 362 | Windows10 Computer Settings | TWGCB-01-005-0362 | 系統\登入 | 關閉圖片密碼登入 | * 此項原則設定可以控制是否讓網域使用者使用圖片密碼登入 * 如果啟用此項原則設定，網域使用者將無法設定或使用圖片密碼登入 * 如果停用或未設定此項原則設定，則網域使用者可以設定並使用圖片密碼 * 請注意，使用這個功能時，使用者的網域密碼會在系統保存庫中快取 | 電腦設定\系統管理範本\系統\登入\關閉圖片密碼登入 | 啟用 |  |
| 363 | Windows10 Computer Settings | TWGCB-01-005-0363 | 系統\OS原則 | 允許在裝置之間的剪貼簿同步處理 | * 此項原則設定決定是否能在裝置上同步剪貼簿內容 * 如果啟用此項原則設定，剪貼簿內容可在已登入相同Microsoft帳戶或Azure AD帳戶的裝置中同步處理 * 如果停用此項原則設定，剪貼簿內容則無法分享到其他裝置上 * 此項原則設定變更後會立即生效 | 電腦設定\系統管理範本\系統\OS原則\允許在裝置之間的剪貼簿同步處理 | 停用 |  |
| 364 | Windows10 Computer Settings | TWGCB-01-005-0364 | 系統\OS原則 | 允許上傳使用者活動 | * 此項原則設定決定是否可以上傳公布的使用者活動 * 如果啟用此原則設定，即允許上傳「使用者活動」的活動類型 * 如果停用此原則設定，則不允許上傳「使用者活動」的活動類型 * 刪除「使用者活動」的活動類型與此設定無關 * 此項原則設定變更後會立即生效 | 電腦設定\系統管理範本\系統\OS原則\允許上傳使用者活動 | 停用 |  |
| 365 | Windows10 Computer Settings | TWGCB-01-005-0365 | Windows元件 | 允許Windows應用程式在系統鎖定時透過語音啟動 | * 此項原則設定決定Windows應用程式在系統鎖定時是否可以透過語音啟動 * 若選擇使用者控制選項，則使用者可在裝置上使用「設定」>「隱私權」，來決定使用者是否能在裝置鎖定時使用語音來與應用程式互動 * 若選擇強制允許選項，則使用者可在系統鎖定時透過語音來與應用程式互動，且使用者無法加以變更 * 若選擇強制拒絕選項，則使用者無法在系統鎖定時透過語音來與應用程式互動，且使用者無法加以變更 * 若停用或未設定此項原則設定，則使用者可在裝置上使用「設定」>「隱私權」，來決定使用者是否可在系統鎖定時使用語音來與應用程式互動 * 此原則會套用到Windows應用程式與Cortana。此原則會優先於允許在鎖定時使用Cortana原則。只有在允許語音啟動原則設定為允許透過語音啟動應用程式時，才適用此原則 | 電腦設定\系統管理範本\Windows元件\App隱私\允許Windows應用程式在系統鎖定時透過語音啟動 | 啟用，強制拒絕 |  |
| 366 | Windows10 Computer Settings | TWGCB-01-005-0366 | Windows | 允許簡訊服務雲端同步 | 此項原則設定決定是否允許將行動數據簡訊備份及還原到Microsoft雲端服務 | 電腦設定\系統管理範本\Windows元件\訊息中心\允許簡訊服務雲端同步 | 停用 |  |
| 367 | Windows10 Computer Settings | TWGCB-01-005-0367 | Windows元件 | 允許雲端搜尋 | * 此項原則設定決定是否允許搜尋，並允許Cortana搜尋雲端來源，例如OneDrive與SharePoint * 啟用時，此項原則設定將雲端搜尋設定限制為以下設定： * 停用雲端搜尋 * 啟用雲端搜尋 * 已選取使用者 | 電腦設定\系統管理範本\Windows元件\搜尋\允許雲端搜尋 | 啟用，雲端搜尋設定：停用雲端搜尋 |  |
| 368 | Windows10 Computer Settings | TWGCB-01-005-0368 | Windows元件 | 允許在鎖定畫面上使用Cortana | * 此項原則設定決定使用者是否可以在系統鎖定時使用語音與Cortana互動 * 若啟用或未設定此項原則設定，使用者可以在系統鎖定時使用語音與Cortana互動 * 若停用此項原則設定，使用者必須將系統解除鎖定，才能使用語音與Cortana互動 | 電腦設定\系統管理範本\Windows元件\搜尋\允許在鎖定畫面上使用Cortana | 停用 |  |
| 369 | Windows10 Computer Settings | TWGCB-01-005-0369 | Windows元件 | 只在Microsoft Store中顯示私人市集 | * 此項原則設定決定是否在Microsoft Store中僅顯示私人市集，禁止存取零售型錄 * 若啟用此項原則設定，使用者將無法在Microsoft Store中檢視零售型錄，但將能檢視私人市集中的應用程式 * 若停用或未設定此項原則設定，使用者將可以在Microsoft Store中存取零售型錄 | 電腦設定\系統管理範本\Windows元件\市集\只在Microsoft Store中顯示私人市集 | 啟用 |  |
| 370 | Windows10 Computer Settings | TWGCB-01-005-0370 | Windows元件 | 允許Windows Ink工作區中建議的App | 此項原則設定決定是否允許Windows Ink工作區中建議的App | 電腦設定\系統管理範本\Windows元件\Windows Ink工作區\允許Windows Ink工作區中建議的App | 停用 |  |
| 371 | Windows10 Computer Settings | TWGCB-01-005-0371 | Windows元件 | 允許Windows Ink工作區 | 此項原則設定決定是否允許Windows Ink工作區 | 電腦設定\系統管理範本\Windows元件\Windows Ink工作區\允許Windows Ink工作區 | 啟用，選擇下列其中一個動作：開啟，但不允許在鎖定畫面上存取 |  |
| 372 | Windows10 Computer Settings | TWGCB-01-005-0372 | Windows元件 | 啟用或停用Windows遊戲錄影和廣播 | * 此項原則設定可啟用或停用Windows遊戲錄影與廣播功能 * 如果停用此設定，將不允許Windows遊戲錄影 * 如果啟用或未設定此項原則設定，將允許錄影與廣播(串流) | 電腦設定\系統管理範本\Windows元件\Windows遊戲錄影和廣播\啟用或停用Windows遊戲錄影和廣播 | 停用 |  |
| 373 | Windows10 Computer Settings | TWGCB-01-005-0373 | Windows元件 | 需要對遠端(RDP)連線使用特定的安全層 | * 此項原則設定指定在遠端桌面通訊協定 (RDP)連線期間，是否必須使用特定的安全性階層，來確保用戶端與RD工作階段主機伺服器之間的通訊安全 * 如果啟用此項原則設定，在遠端連線期間，用戶端與RD工作階段主機伺服器之間的所有通訊都必須使用這個設定中指定的安全性方法。可用的安全性方法如下： * 交涉：交涉方法會強制執行用戶端支援的最安全方法。如果支援傳輸層安全性(TLS)1.0版，就使用它來驗證RD工作階段主機伺服器。如果不支援TLS，則使用原始遠端桌面通訊協定(RDP)加密來確保通訊安全，但不會驗證RD工作階段主機伺服器。不建議使用原始RDP加密(相對於SSL加密) * RDP：RDP方法會使用原始RDP加密，確保用戶端與RD工作階段主機伺服器之間的通訊安全。如果選取這個設定，就不會驗證RD工作階段主機伺服器。不建議使用原始RDP加密(相對於SSL加密) * SSL(TLS 1.0)：SSL方法必須使用TLS 1.0，來驗證RD工作階段主機伺服器。如果不支援TLS，連線會失敗。這是此原則的建議設定 * 如果停用或未設定此項原則設定，則不會在群組原則層級指定RD工作階段主機伺服器在遠端連線所要使用的安全性方法 | 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\需要對遠端(RDP)連線使用特定的安全層 | 啟用：SSL |  |
| 374 | Windows10 Computer Settings | TWGCB-01-005-0374 | Windows元件 | 透過使用網路層級驗證以要求對遠端連線進行使用者驗證 | * 此項原則設定決定是否要使用網路層級驗證來對連至遠端桌面工作階段主機伺服器的遠端連線要求使用者驗證。此項原則設定要求使用者驗證在遠端連線處理程序初期執行，以增強安全性 * 如果啟用此項原則設定，只有支援網路層級驗證的用戶端電腦能夠連線到遠端桌面工作階段主機伺服器，若要判斷用戶端電腦是否支援網路層級驗證，請在用戶端電腦上啟動「遠端桌面連線」，按一下「遠端桌面連線」對話方塊左上角的圖示，然後按一下「關於」。在「關於遠端桌面連線」對話方塊中，尋找是否出現「支援網路層級驗證」 * 如果停用此項原則設定，則在允許遠端連線到遠端桌面工作階段主機伺服器之前，不必使用網路層級驗證進行使用者驗證 * 如果未設定此項原則設定，則將強制執行目標電腦上的本機設定 * 注意：停用此項原則設定將提供較低的安全性，因為使用者驗證將在遠端連線處理程序後期執行 | 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\透過使用網路層級驗證以要求對遠端連線進行使用者驗證 | 啟用 |  |
| 375 | Windows10 Computer Settings | TWGCB-01-005-0375 | Windows元件 | 防止非系統管理員使用者安裝Windows應用程式套件 | * 此項原則設定決定非系統管理員使用者是否可以安裝Windows應用程式套件 * 如果啟用此項原則設定，非系統管理員將無法啟動Windows應用程式套件的安裝。欲安裝應用程式的系統管理員需要從系統管理員內容(如系統管理員PowerShell視窗)執行此操作。如果其他原則允許，所有使用者仍可以透過Microsoft Store安裝Windows應用程式套件 * 如果停用或未設定此項原則設定，則所有使用者都可以啟動Windows應用程式套件的安裝 | 電腦設定\系統管理範本\Windows元件\應用程式套件部署\防止非系統管理員使用者安裝Windows應用程式套件 | 啟用 |  |
| 376 | Windows10 Computer Settings | TWGCB-01-005-0376 | Windows元件 | 封鎖所有消費者Microsoft 帳戶使用者驗證 | * 此項原則設定負責控制使用者是否能透過提供Microsoft帳戶，進行應用程式或服務的身分驗證 * 如果啟用此原則設定，此裝置上所有應用程式與服務都無法透過Microsoft帳戶進行身分驗證 * 此設定同時適用於裝置目前的使用者以及可能新增的新使用者。但是對於已驗證使用者的應用程式或服務，在身分快取驗證過期前，啟用此設定將不會造成任何影響 * 建議在任何使用者登入裝置前啟用此原則設定，避免快取權杖出現。如果停用或未設定原則此設定，應用程式與服務可以使用Microsoft帳戶進行身分驗證 * 在預設情況下，此設定將被停用。此設定不影響使用者是否能透過Microsoft帳戶登入裝置，或使用者透過瀏覽器提供Microsoft帳戶以進行Web架構應用程式身分驗證的能力 | 電腦設定\系統管理範本\Windows元件\Microsoft帳戶\封鎖所有消費者Microsoft帳戶使用者驗證 | 啟用 |  |
| 377 | Windows10 Computer Settings | TWGCB-01-005-0377 | 安全性選項\網路存取 | 網路存取：限制允許對SAM發出遠端呼叫的用戶端 | * 此項原則設定可限制使用者對SAM的遠端RPC連線 * 若未選取，將會使用預設安全性描述元 | 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：限制允許對SAM發出遠端呼叫的用戶端 | 選擇Administrators群組，並勾選允許遠端存取 |  |
| 378 | Windows10 Computer Settings | TWGCB-01-005-0378 | 網路\網路連線 | 禁止在您的DNS網域網路中使用網際網路連線共用 | * 此項原則設定決定是否使用行動熱點功能 * 如果啟用此項原則設定，管理員與非管理員都無法啟用或設定行動熱點功能 * 如果停用或未設定此項原則設定，使用者可以設定行動熱點功能 * 注意：此在舊版的Windows作業系統為網際網路連線共用(Internet Connection Sharing, ICS)功能 | 電腦設定\系統管理範本\網路\網路連線\禁止在您的DNS網域網路中使用網際網路連線共用 | 啟用 |  |
| 379 | Windows10 Computer Settings | TWGCB-01-005-0379 | 系統\認證委派 | 遠端主機允許委派不可匯出的認證 | * 使用認證委派時，裝置會將可匯出版本的認證提供給遠端主機。這會讓使用者暴露在遠端主機上攻擊者偷取認證的風險下 * 若啟用此項原則設定，主機支援「受限的系統管理」或Remote Credential Guard 模式 * 若停用或未設定此項原則設定，則不支援「受限的系統管理」與Remote Credential Guard模式。使用者一律需要將其認證傳遞給主機 | 電腦設定\系統管理範本\系統\認證委派\遠端主機允許委派不可匯出的認證 | 啟用 |  |
| 380 | Windows10 User Settings | TWGCB-01-005-0380 | Windows元件 | 開啟或關閉詳細資料窗格 | * 此項原則設定決定是否在「檔案總管」中顯示或隱藏「詳細資料」窗格 * 如果啟用此項原則設定並設定為隱藏窗格，就會隱藏「檔案總管」中的「詳細資料」窗格，且使用者無法將其開啟 * 如果啟用此項原則設定並設定為顯示窗格，就一律會顯示「檔案總管」中的「詳細資料」窗格，且使用者無法將其隱藏。這個設定的副作用是無法切換成「預覽」窗格，因為「詳細資料」窗格不能和「預覽」窗格同時顯示 * 如果停用或未設定此項原則設定，則會依預設隱藏「詳細資料」窗格，且使用者可以將其顯示，這是預設的原則設定 | 使用者設定\系統管理範本\Windows元件\檔案總管\檔案總管框架窗格\開啟或關閉詳細資料窗格 | 啟用：一律隱藏 |  |
| 381 | Windows10 User Settings | TWGCB-01-005-0381 | Windows元件 | 關閉預覽窗格 | * 此項原則設定決定是否隱藏「檔案總管」中的「預覽」窗格 * 如果啟用此項原則設定，就會隱藏「檔案總管」中的「預覽」窗格，且使用者無法將其開啟 * 如果停用或未設定此項原則設定，則會依預設隱藏「預覽」窗格，但使用者可以將其顯示 | 使用者設定\系統管理範本\Windows元件\檔案總管\檔案總管框架窗格\關閉預覽窗格 | 啟用 |  |
| 本中心整理 | | | | | | | | |

# 參考文獻

1. Common Configuration Enumeration(CCE)List.

http：//cce.mitre.org/lists/cce\_list.html

1. Windows 10 Version 2004 and Windows Server Version 2004 Security Baseline.

https://www.microsoft.com/en-us/download/details.aspx?id=55319

1. Center for Internet Security, CIS Microsoft Windows 10 Enterprise (Release 2004) Benchmark v1.9.1.

https://www.cisecurity.org/cis-benchmarks/

1. Defense Information Systems Agency (DISA), Windows 10 STIG Version: 1 Release: 23.

https://public.cyber.mil/stigs/downloads/

# 附件

附件1版次1.4異動設定項目列表

1. 版次1.4異動設定項目列表

* 新增列表

| 項次 | GPO | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | GPO設定路徑 | GCB設定值 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Windows10 Computer Settings | TWGCB-01-005-0346 | 進階稽核原則設定 | 稽核詳細的檔案共用 | * 此項原則設定可稽核存取共用資料夾中之檔案及資料夾的嘗試，記錄每次存取檔案或資料夾的事件，包括關於權限或用來授與或拒絕存取之其他條件的詳細資訊 * 如果設定此項原則設定，當嘗試存取共用上的檔案或資料夾時，就會產生稽核事件。系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 * 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用此項原則設定，則會稽核系統上所有共用檔案與資料夾的存取 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核詳細的檔案共用 | 失敗 |
| 2 | Windows10 Computer Settings | TWGCB-01-005-0347 | 進階稽核原則設定 | 稽核檔案共用 | * 此項原則設定可稽核存取共用資料夾的嘗試 * 如果設定此項原則設定，則會在嘗試存取共用資料夾時產生稽核事件。系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 * 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用此項原則設定，則會稽核系統上所有共用資料夾的存取 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核檔案共用 | 成功與失敗 |
| 3 | Windows10 Computer Settings | TWGCB-01-005-0348 | 進階稽核原則設定 | 稽核其他物件存取事件 | * 此項原則設定可稽核因管理工作排程器物件或COM+物件而產生之事件 * 如果是排程器工作，則會稽核下列項目： * 建立工作 * 刪除工作 * 啟用工作 * 停用工作 * 更新工作 * 如果是COM+物件，則會稽核下列項目： * 新增類別目錄物件 * 更新類別目錄物件 * 刪除類別目錄物件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核其他物件存取事件 | 成功與失敗 |
| 4 | Windows10 Computer Settings | TWGCB-01-005-0349 | 進階稽核原則設定 | 稽核授權原則變更 | * 此項原則設定稽核因授權原則變更而產生之事件，例如： * 指派未透過「驗證原則變更」子類別稽核的使用者權限(如SeCreateTokenPrivilege) * 移除未透過「驗證原則變更」子類別稽核的使用者權限(如SeCreateTokenPrivilege) * 加密檔案系統(EFS)原則的變更 * 物件之資源屬性的變更 * 套用至物件之集中存取原則(CAP)的變更 * 如果設定此項原則設定，則會在嘗試變更授權原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更授權原則時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核授權原則變更 | 成功 |
| 5 | Windows10 Computer Settings | TWGCB-01-005-0350 | 進階稽核原則設定 | MPSSVC規則層級原則變更 | * 此項原則設定可稽核因Microsoft保護服務(MPSSVC)使用之原則規則變更而產生之事件。這個服務是供Windows防火牆使用。包含下列事件： * 報告Windows防火牆服務啟動時的使用中原則 * Windows防火牆規則的變更 * Windows防火牆例外清單的變更 * Windows防火牆設定的變更 * Windows防火牆服務忽略或未套用的規則 * Windows防火牆群組原則設定的變更 * 如果設定此項原則設定，則會在嘗試變更MPSSVC所使用的原則規則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，在MPSSVC使用的原則規則變更時則不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\MPSSVC規則層級原則變更 | 成功與失敗 |
| 6 | Windows10 Computer Settings | TWGCB-01-005-0351 | 進階稽核原則設定 | 稽核其他原則變更事件 | * 此項原則設定可稽核原則變更類別未稽核之其他安全性原則變更所產生的稽核事件，例如： * 信賴平台模組(TPM)設定變更 * 核心模式密碼編譯自我測試 * 密碼編譯提供者操作 * 密碼編譯內容操作或修改 * 套用的集中存取原則(CAP)變更 * 開機設定資料(BCD)修改 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核其他原則變更事件 | 失敗 |
| 7 | Windows10 Computer Settings | TWGCB-01-005-0352 | 進階稽核原則設定 | 稽核PNP活動 | * 此項原則設定可在隨插即用偵測到外接式裝置時執行稽核 * 若設定此項原則設定，每當隨插即用偵測到外接式裝置時會產生稽核事件。此類別只會記錄成功稽核 * 若未設定此項原則設定，當隨插即用偵測到外接式裝置時不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核PNP活動 | 成功 |
| 8 | Windows10 Computer Settings | TWGCB-01-005-0353 | 進階稽核原則設定 | 稽核群組成員資格 | * 此項原則可稽核使用者登入權杖中的群組成員資格資訊。這個子類別中的事件會在建立登入工作階段的電腦上產生。對於互動式登入，安全性稽核事件會在使用者登入的電腦上產生。對於網路登入(例如存取網路上的共用資料夾)，安全性稽核事件會在主控資源的電腦上產生 * 設定此設定後，會針對每個成功的登入產生一或多個安全性稽核事件，且必須啟用「進階稽核原則設定\系統稽核原則\登入/登出」底下的「稽核登入」設定。如果單一安全性稽核事件無法容納群組成員資格資訊，則會產生多個事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核群組成員資格 | 成功 |
| 9 | Windows10 Computer Settings | TWGCB-01-005-0354 | 進階稽核原則設定 | 稽核其他登入/登出事件 | * 此項原則設定可稽核「登入/登出」原則設定未涵蓋之其他登入/登出相關事件，例如： * 終端機服務工作階段中斷連線 * 新的終端機服務工作階段 * 鎖定及解除鎖定工作站 * 呼叫螢幕保護裝置 * 解除螢幕保護裝置 * 偵測Kerberos重新執行攻擊，在這類攻擊中，會接收到具有相同資訊的Kerberos要求2次。這個狀況可能是網路設定錯誤而造成 * 將無線網路存取權限授與使用者或電腦帳戶 * 將有線802.1x網路存取權限授與使用者或電腦帳戶 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核其他登入/登出事件 | 成功與失敗 |
| 10 | Windows10 Computer Settings | TWGCB-01-005-0355 | 控制台 | 允許線上提示 | * 此項原則設定可啟用或停用擷取「設定」應用程式的線上提示與說明 * 若停用此項原則設定，「設定」將不會連絡Microsoft內容服務來擷取提示與說明內容 | 電腦設定\系統管理範本\控制台\允許線上提示 | 停用 |
| 11 | Windows10 Computer Settings | TWGCB-01-005-0356 | MS Security Guide | Configure SMB v1 client driver | * 停用用戶端SMBv1協定，請選擇「啟用」，並於Configure MrxSmb10 driver下拉選項中，選擇「Disable driver(recommended)」 * 警告：任何狀況下請不要選擇停用選項 * 對於Windows 7、Servers 2008、2008R2及2012作業系統，須額外設定「Configure SMB v1 client」設定 * 要復原預設用戶端的SMBv1設定，請選擇請選擇「啟用」，並於Configure MrxSmb10 driver中選擇正確的預設值 * 針對Windows 7、Windows Server 2008、2008R2及2012版本請選擇「手動啟動」 * 針對Windows 8.1、Windows Server 2012R2及更高版本請選擇「自動啟動」 * 此設定所做的更改需要重新啟動才能生效 | 電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 client driver | 啟用，Configure MrxSmb10 driver：Disable driver(recommended) |
| 12 | Windows10 Computer Settings | TWGCB-01-005-0357 | MS Security Guide | Configure SMB v1 server | * 停用此設定將停用伺服器端SMBv1協定的處理(推薦) * 啟用此設定將啟用伺服器端SMBv1協定的處理(預設) * 此設定所做的更改需要重新啟動才能生效 | 電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 server | 停用 |
| 13 | Windows10 Computer Settings | TWGCB-01-005-0358 | MS Security Guide | Enable Structured Exception Handling Overwrite Protection (SEHOP) | * 如果啟用此原則，則將強制執行SEHOP * 如果停用或未設定此原則，則對於32位元處理器將不強制執行SEHOP | 電腦設定\系統管理範本\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP) | 啟用 |
| 14 | Windows10 Computer Settings | TWGCB-01-005-0359 | MS Security Guide | NetBT NodeType configuration | * NetBT NodeType設定決定NetBT用於註冊與解析名稱的方法： * B節點電腦使用廣播 * P節點電腦僅使用對名稱伺服器(WINS)的點對點名稱查詢 * M節點電腦先廣播，然後查詢名稱伺服器 * H節點電腦先查詢名稱伺服器，然後廣播 * 遵循以下方法通過LMHOSTS或DNS進行解析。如果存在NodeType值，它將覆蓋任何DhcpNodeType值 * 如果沒有NodeType與DhcpNodeType，也沒有WINS伺服器，電腦使用B節點，如果至少設定了WINS伺服器，則電腦使用H節點 | 電腦設定\系統管理範本\MS Security Guide\NetBT NodeType configuration | 啟用，Configure NetBT NodeType：P節點(推薦) |
| 15 | Windows10 Computer Settings | TWGCB-01-005-0360 | 網路\DNS用戶端 | 關閉多點傳送名稱解析 | * 此項原則設定可啟用或停用連結本機多點傳送名稱解析(LLMNR) * LLMNR是次要名稱解析通訊協定。使用LLMNR，查詢會透過單一子網路的本機網路連結，使用多點傳送從一部用戶端電腦傳送到相同子網路上同時啟用LLMNR的另一部用戶端電腦，LLMNR不需要DNS伺服器或DNS用戶端設定，可針對無法透過傳統DNS名稱解析的狀況提供名稱解析 * 如果啟用此項原則設定，會停用用戶端電腦上所有可用的網路介面卡之LLMNR * 如果停用或未設定此項原則設定，會啟用所有可用的網路介面卡之LLMNR | 電腦設定\系統管理範本\網路\DNS用戶端\關閉多點傳送名稱解析 | 啟用 |
| 16 | Windows10 Computer Settings | TWGCB-01-005-0361 | 系統\認證委派 | 加密預示修復 | * 此項原則設定適用於使用CredSSP元件之應用程式(例如遠端桌面連線) * CredSSP通訊協定的某些版本有弱點，容易受到針對用戶端的加密Oracle攻擊所威脅。此項原則會控制易受攻擊的用戶端與伺服器的相容性，可設定加密預示弱點所需的保護層級 * 如果啟用此項原則設定，就會依據下列選項來選取CredSSP版本支援：   + 強制使用更新的用戶端：使用CredSSP的用戶端應用程式將無法回復成不安全的版本，並且使用CredSSP的服務將不會接受未修補的用戶端。注意：除非所有遠端主機都已支援最新的版本，否則不應該部署此項設定   + 已降低影響：使用CredSSP的用戶端應用程式將無法回復成不安全的版本，但使用CredSSP的服務可接受未修補的用戶端   + 易受攻擊：使用CredSSP的用戶端應用程式可支援回復成不安全的版本，且使用CredSSP的服務可接受未修補的用戶端，進而導致遠端伺服器容易遭受攻擊 | 電腦設定\系統管理範本\系統\認證委派\加密預示修復 | 啟用，保護層級：強制使用更新的用戶端 |
| 17 | Windows10 Computer Settings | TWGCB-01-005-0362 | 系統\登入 | 關閉圖片密碼登入 | * 此項原則設定可以控制是否讓網域使用者使用圖片密碼登入 * 如果啟用此項原則設定，網域使用者將無法設定或使用圖片密碼登入 * 如果停用或未設定此項原則設定，則網域使用者可以設定並使用圖片密碼 * 請注意，使用這個功能時，使用者的網域密碼會在系統保存庫中快取 | 電腦設定\系統管理範本\系統\登入\關閉圖片密碼登入 | 啟用 |
| 18 | Windows10 Computer Settings | TWGCB-01-005-0363 | 系統\OS原則 | 允許在裝置之間的剪貼簿同步處理 | * 此項原則設定決定是否能在裝置上同步剪貼簿內容 * 如果啟用此項原則設定，剪貼簿內容可在已登入相同Microsoft帳戶或Azure AD帳戶的裝置中同步處理 * 如果停用此項原則設定，剪貼簿內容則無法分享到其他裝置上 * 此項原則設定變更後會立即生效 | 電腦設定\系統管理範本\系統\OS原則\允許在裝置之間的剪貼簿同步處理 | 停用 |
| 19 | Windows10 Computer Settings | TWGCB-01-005-0364 | 系統\OS原則 | 允許上傳使用者活動 | * 此項原則設定決定是否可以上傳公布的使用者活動 * 如果啟用此原則設定，即允許上傳「使用者活動」的活動類型 * 如果停用此原則設定，則不允許上傳「使用者活動」的活動類型 * 刪除「使用者活動」的活動類型與此設定無關 * 此項原則設定變更後會立即生效 | 電腦設定\系統管理範本\系統\OS原則\允許上傳使用者活動 | 停用 |
| 20 | Windows10 Computer Settings | TWGCB-01-005-0365 | Windows元件 | 允許Windows應用程式在系統鎖定時透過語音啟動 | * 此項原則設定決定Windows應用程式在系統鎖定時是否可以透過語音啟動 * 若選擇使用者控制選項，則使用者可在裝置上使用「設定」>「隱私權」，來決定使用者是否能在裝置鎖定時使用語音來與應用程式互動 * 若選擇強制允許選項，則使用者可在系統鎖定時透過語音來與應用程式互動，且使用者無法加以變更 * 若選擇強制拒絕選項，則使用者無法在系統鎖定時透過語音來與應用程式互動，且使用者無法加以變更 * 若停用或未設定此項原則設定，則使用者可在裝置上使用「設定」>「隱私權」，來決定使用者是否可在系統鎖定時使用語音來與應用程式互動 * 此原則會套用到Windows應用程式與Cortana。此原則會優先於允許在鎖定時使用Cortana原則。只有在允許語音啟動原則設定為允許透過語音啟動應用程式時，才適用此原則 | 電腦設定\系統管理範本\Windows元件\App隱私\允許Windows應用程式在系統鎖定時透過語音啟動 | 啟用，強制拒絕 |
| 21 | Windows10 Computer Settings | TWGCB-01-005-0366 | Windows元件 | 允許簡訊服務雲端同步 | 此項原則設定決定是否允許將行動數據簡訊備份及還原到Microsoft雲端服務 | 電腦設定\系統管理範本\Windows元件\訊息中心\允許簡訊服務雲端同步 | 停用 |
| 22 | Windows10 Computer Settings | TWGCB-01-005-0367 | Windows元件 | 允許雲端搜尋 | 此項原則設定決定是否允許搜尋，並允許Cortana搜尋雲端來源，例如OneDrive與SharePoint | 電腦設定\系統管理範本\Windows元件\搜尋\允許雲端搜尋 | 啟用，雲端搜尋設定：停用雲端搜尋 |
| 23 | Windows10 Computer Settings | TWGCB-01-005-0368 | Windows元件 | 允許在鎖定畫面上使用Cortana | * 此項原則設定決定使用者是否可以在系統鎖定時使用語音與Cortana互動 * 若啟用或未設定此項原則設定，使用者可以在系統鎖定時使用語音與Cortana互動 * 若停用此項原則設定，使用者必須將系統解除鎖定，才能使用語音與Cortana互動 | 電腦設定\系統管理範本\Windows元件\搜尋\允許在鎖定畫面上使用Cortana | 停用 |
| 24 | Windows10 Computer Settings | TWGCB-01-005-0369 | Windows元件 | 只在Microsoft Store中顯示私人市集 | * 此項原則設定決定是否在Microsoft Store中僅顯示私人市集，禁止存取零售型錄 * 若啟用此項原則設定，使用者將無法在Microsoft Store中檢視零售型錄，但將能檢視私人市集中的應用程式 * 若停用或未設定此項原則設定，使用者將可以在Microsoft Store中存取零售型錄 | 電腦設定\系統管理範本\Windows元件\市集\只在Microsoft Store中顯示私人市集 | 啟用 |
| 25 | Windows10 Computer Settings | TWGCB-01-005-0370 | Windows元件 | 允許Windows Ink工作區中建議的App | 此項原則設定決定是否允許Windows Ink工作區中建議的App | 電腦設定\系統管理範本\Windows元件\Windows Ink工作區\允許Windows Ink工作區中建議的App | 停用 |
| 26 | Windows10 Computer Settings | TWGCB-01-005-0371 | Windows元件 | 允許Windows Ink工作區 | 此項原則設定決定是否允許Windows Ink工作區 | 電腦設定\系統管理範本\Windows元件\Windows Ink工作區\允許Windows Ink工作區 | 啟用，選擇下列其中一個動作：開啟，但不允許在鎖定畫面上存取 |
| 27 | Windows10 Computer Settings | TWGCB-01-005-0372 | Windows元件 | 啟用或停用Windows遊戲錄影和廣播 | * 此項原則設定可啟用或停用Windows遊戲錄影與廣播功能 * 如果停用此設定，將不允許Windows遊戲錄影 * 如果啟用或未設定此項原則設定，將允許錄影與廣播(串流) | 電腦設定\系統管理範本\Windows元件\Windows遊戲錄影和廣播\啟用或停用Windows遊戲錄影和廣播 | 停用 |
| 28 | Windows10 Computer Settings | TWGCB-01-005-0373 | Windows元件 | 需要對遠端(RDP)連線使用特定的安全層 | * 此項原則設定指定在遠端桌面通訊協定(RDP)連線期間，是否必須使用特定的安全性階層，來確保用戶端與RD工作階段主機伺服器之間的通訊安全 * 如果啟用此項原則設定，在遠端連線期間，用戶端與RD工作階段主機伺服器之間的所有通訊都必須使用這個設定中指定的安全性方法。可用的安全性方法如下：   + 交涉：交涉方法會強制執行用戶端支援的最安全方法。如果支援傳輸層安全性(TLS)1.0版，就使用它來驗證RD工作階段主機伺服器。如果不支援TLS，則使用原始遠端桌面通訊協定(RDP)加密來確保通訊安全，但不會驗證RD工作階段主機伺服器。不建議使用原始RDP加密(相對於SSL加密)   + RDP：RDP方法會使用原始RDP加密，確保用戶端與RD工作階段主機伺服器之間的通訊安全。如果選取這個設定，就不會驗證RD工作階段主機伺服器。不建議使用原始RDP加密(相對於SSL加密)   + SSL(TLS 1.0)：SSL方法必須使用TLS 1.0，來驗證RD工作階段主機伺服器。如果不支援TLS，連線會失敗。這是此原則的建議設定 * 如果停用或未設定此項原則設定，則不會在群組原則層級指定RD工作階段主機伺服器在遠端連線所要使用的安全性方法 | 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\需要對遠端(RDP)連線使用特定的安全層 | 啟用：SSL |
| 29 | Windows10 Computer Settings | TWGCB-01-005-0374 | Windows元件 | 透過使用網路層級驗證以要求對遠端連線進行使用者驗證 | * 此項原則設定決定是否要使用網路層級驗證來對連至遠端桌面工作階段主機伺服器的遠端連線要求使用者驗證。此項原則設定要求使用者驗證在遠端連線處理程序初期執行，以增強安全性 * 如果啟用此項原則設定，只有支援網路層級驗證的用戶端電腦能夠連線到遠端桌面工作階段主機伺服器，若要判斷用戶端電腦是否支援網路層級驗證，請在用戶端電腦上啟動「遠端桌面連線」，按一下「遠端桌面連線」對話方塊左上角的圖示，然後按一下「關於」。在「關於遠端桌面連線」對話方塊中，尋找是否出現「支援網路層級驗證」 * 如果停用此項原則設定，則在允許遠端連線到遠端桌面工作階段主機伺服器之前，不必使用網路層級驗證進行使用者驗證 * 如果未設定此項原則設定，則將強制執行目標電腦上的本機設定。在Windows Server 2012與Windows 8中，預設會強制執行網路層級驗證 * 注意：停用此項原則設定將提供較低的安全性，因為使用者驗證將在遠端連線處理程序後期執行 | 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\透過使用網路層級驗證以要求對遠端連線進行使用者驗證 | 啟用 |
| 30 | Windows10 Computer Settings | TWGCB-01-005-0375 | Windows元件 | 防止非系統管理員使用者安裝Windows應用程式套件 | * 此項原則設定決定非系統管理員使用者是否可以安裝Windows應用程式套件 * 如果啟用此項原則設定，非系統管理員將無法啟動Windows應用程式套件的安裝。欲安裝應用程式的系統管理員需要從系統管理員內容(如系統管理員PowerShell視窗)執行此操作。如果其他原則允許，所有使用者仍可以透過Microsoft Store安裝Windows應用程式套件 * 如果停用或未設定此項原則設定，則所有使用者都可以啟動Windows應用程式套件的安裝 | 電腦設定\系統管理範本\Windows元件\應用程式套件部署\防止非系統管理員使用者安裝Windows應用程式套件 | 啟用 |
| 31 | Windows10 Computer Settings | TWGCB-01-005-0376 | Windows元件 | 封鎖所有消費者Microsoft帳戶使用者驗證 | * 此項原則設定負責控制使用者是否能透過提供Microsoft帳戶，進行應用程式或服務的身分驗證 * 如果啟用此原則設定，此裝置上所有應用程式與服務都無法透過Microsoft帳戶進行身分驗證 * 此設定同時適用於裝置目前的使用者以及可能新增的新使用者。但是對於已驗證使用者的應用程式或服務，在身分快取驗證過期前，啟用此設定將不會造成任何影響 * 建議在任何使用者登入裝置前啟用此原則設定，避免快取權杖出現。如果停用或未設定原則此設定，應用程式與服務可以使用Microsoft帳戶進行身分驗證 * 在預設情況下，此設定將被停用。此設定不影響使用者是否能透過Microsoft帳戶登入裝置，或使用者透過瀏覽器提供Microsoft帳戶以進行Web架構應用程式身分驗證的能力 | 電腦設定\系統管理範本\Windows元件\Microsoft帳戶\封鎖所有消費者Microsoft帳戶使用者驗證 | 啟用 |
| 32 | Windows10 Computer Settings | TWGCB-01-005-0377 | 安全性選項\網路存取 | 網路存取：限制允許對SAM發出遠端呼叫的用戶端 | * 此項原則設定可限制使用者對SAM的遠端RPC連線 * 若未選取，將會使用預設安全性描述元 | 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：限制允許對SAM發出遠端呼叫的用戶端 | 選擇Administrators群組，並勾選允許遠端存取 |
| 33 | Windows10 Computer Settings | TWGCB-01-005-0378 | 網路\網路連線 | 禁止在您的DNS網域網路中使用網際網路連線共用 | * 此為舊版設定，適用於傳統Windows 2000、Windows XP及Server 2003中的網際網路連線共用(Internet Connection Sharing, ICS)功能，現在此功能適用於Windows 10與Server 2016的行動熱點功能 * 如果啟用此項原則設定，管理員與非管理員都無法啟用或設定行動熱點功能 * 如果停用或未設定此項原則設定，使用者可以設定行動熱點功能 | 電腦設定\系統管理範本\網路\網路連線\禁止在您的DNS網域網路中使用網際網路連線共用 | 啟用 |
| 34 | Windows10 Computer Settings | TWGCB-01-005-0379 | 系統\認證委派 | 遠端主機允許委派不可匯出的認證 | * 使用認證委派時，裝置會將可匯出版本的認證提供給遠端主機。這會讓使用者暴露在遠端主機上攻擊者偷取認證的風險下 * 若啟用此項原則設定，主機支援「受限的系統管理」或Remote Credential Guard模式 * 若停用或未設定此項原則設定，則不支援「受限的系統管理」與Remote Credential Guard模式。使用者一律需要將其認證傳遞給主機 | 電腦設定\系統管理範本\系統\認證委派\遠端主機允許委派不可匯出的認證 | 啟用 |
| 35 | Windows10 User Settings | TWGCB-01-005-0380 | Windows元件 | 開啟或關閉詳細資料窗格 | * 此項原則設定決定是否在「檔案總管」中顯示或隱藏「詳細資料」窗格 * 如果啟用此項原則設定並設定為隱藏窗格，就會隱藏「檔案總管」中的「詳細資料」窗格，且使用者無法將其開啟 * 如果啟用此項原則設定並設定為顯示窗格，就一律會顯示「檔案總管」中的「詳細資料」窗格，且使用者無法將其隱藏。這個設定的副作用是無法切換成「預覽」窗格，因為「詳細資料」窗格不能和「預覽」窗格同時顯示 * 如果停用或未設定此項原則設定，則會依預設隱藏「詳細資料」窗格，且使用者可以將其顯示，這是預設的原則設定 | 使用者設定\系統管理範本\Windows元件\檔案總管\檔案總管框架窗格\開啟或關閉詳細資料窗格 | 啟用：一律隱藏 |
| 36 | Windows10 User Settings | TWGCB-01-005-0381 | Windows元件 | 關閉預覽窗格 | * 此項原則設定決定是否隱藏「檔案總管」中的「預覽」窗格 * 如果啟用此項原則設定，就會隱藏「檔案總管」中的「預覽」窗格，且使用者無法將其開啟 * 如果停用或未設定此項原則設定，則會依預設隱藏「預覽」窗格，但使用者可以將其顯示 | 使用者設定\系統管理範本\Windows元件\檔案總管\檔案總管框架窗格\關閉預覽窗格 | 啟用 |
| 本中心整理 | | | | | | | |

* 修改列表

| 項次 | 修改對照 | GPO | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | GPO設定路徑 | GCB設定值 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0002 | 帳戶原則\密碼原則 | 密碼最長使用期限 | * 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在1至999天之後到期；或將天數設為0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於1到999天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以是介於0到998天之間的任何數值 * 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每30至90天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限 * 注意：若使用者帳戶啟用「密碼永久有效」設定，將覆蓋此原則設定，導致系統不會要求該使用者變更密碼，即該使用者帳戶之密碼永遠不會到期 | 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 | 90天以下 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0002 | 帳戶原則\密碼原則 | 密碼最長使用期限 | * 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在1至999天之後到期；或將天數設為0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於1到999天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以是介於0到998天之間的任何數值 * 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每30至90天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限 * 注意：若使用者帳戶啟用「密碼永久有效」設定，將覆蓋此原則設定，導致系統不會要求該使用者變更密碼，即該使用者帳戶之密碼永遠不會到期 | 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 | 90天以下，但須大於0天 |
| 2 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0003 | 帳戶原則\密碼原則 | 最小密碼長度 | * 此項原則設定決定使用者帳戶的密碼可包含的最少字元數。可以設定介於1到14個字元之間的值 * 將字元數設為0，則表示不需要密碼 | 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 | 8個字元以上 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0003 | 帳戶原則\密碼原則 | 最小密碼長度 | * 此項原則設定決定使用者帳戶的密碼可包含的最少字元數 * 此設定的最大值取決於「放寬最小密碼長度限制」的設定值 * 如果未定義「放寬最小密碼長度限制」設定，則此設定可以設為0到14 * 如果已定義並停用「放寬最小密碼長度限制」設定，則此設定可以設為0到14 * 如果已定義並啟用「放寬最小密碼長度限制」設定，則此設定可以設為0到128 * 將字元數設為0，則表示不需要密碼 | 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 | 8個字元以上 |
| 3 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0005 | 帳戶原則\密碼原則 | 強制執行密碼歷程記錄 | * 此項原則設定決定重複使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於0與24個密碼之間 * 此項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性 | 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 | 3以上記憶的密碼 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0005 | 帳戶原則\密碼原則 | 強制執行密碼歷程記錄 | * 此項原則設定決定重複使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於0與24個密碼之間 * 此項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性 | 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 | 3個以上記憶的密碼 |
| 4 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0007 | 帳戶原則\帳戶原則 | 帳戶鎖定閾值 | * 這項原則設定決定使用者帳戶被鎖定的嘗試登入失敗次數，除非由系統管理員重設或該帳戶的鎖定期間已到期，否則無法使用該鎖定帳戶 * 可將失敗的登入嘗試值設定為介於0到999之間。如果將值設定為0，將永遠不會鎖定該帳戶 * 針對使用CTRL+ALT+DELETE或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾值 | 5次不正確的登入嘗試 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0007 | 帳戶原則\帳戶原則 | 帳戶鎖定閾值 | * 此項原則設定決定使用者帳戶被鎖定的嘗試登入失敗次數，除非由系統管理員重設或該帳戶的鎖定期間已到期，否則無法使用該鎖定帳戶 * 可將失敗的登入嘗試值設定為介於0到999之間。如果將值設定為0，將永遠不會鎖定該帳戶 * 針對使用CTRL+ALT+DELETE或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾值 | 5次以下不正確的登入嘗試，但須大於0次 |
| 5 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0008 | 帳戶原則\帳戶原則 | 重設帳戶鎖定計數器的時間間隔 | * 此項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入嘗試計數器重設為0次失敗。可用的範圍是從1分鐘到99,999分鐘 * 如果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 | 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 | 15分鐘 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0008 | 帳戶原則\帳戶原則 | 重設帳戶鎖定計數器的時間間隔 | * 此項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入嘗試計數器重設為0次失敗。可用的範圍是從1分鐘到99,999分鐘 * 如果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 | 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 | 15分鐘以上 |
| 6 | 修改前 | Windows10 Account Settings | TWGCB-01-005-0009 | 帳戶原則\帳戶原則 | 帳戶鎖定期間 | * 此項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數 * 設定範圍從0分鐘到99,999分鐘。如果將帳戶鎖定期間設定為0，將會繼續鎖定帳戶，直到系統管理員將該帳戶解除鎖定 * 如果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 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定期間 | 15分鐘 |
| 修改後 | Windows10 Account Settings | TWGCB-01-005-0009 | 帳戶原則\帳戶原則 | 帳戶鎖定期間 | * 此項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數 * 設定範圍從0分鐘到99,999分鐘。如果將帳戶鎖定期間設定為0，將會繼續鎖定帳戶，直到系統管理員將該帳戶解除鎖定 * 如果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 | 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定期間 | 15分鐘以上 |
| 7 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0013 | 網路\網路連線 | 禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | * 此項原則設定決定使用者是否可以安裝及設定網路橋接器 * 注意：此項設定與位置有關。只有當電腦連線到相同DNS網域網路，而且在這個連線上更新設定，才會套用此項設定。如果設定更新之後，電腦又連線到其他不同的DNS網域網路，此項設定將不會生效 * 網路橋接器可以讓使用者建立層級2MAC橋接器，啟用橋接器可以將兩個(含)以上的網路區段連在一起。這個連線會出現在「網路連線」資料夾中 * 如果停用或未設定此項原則設定，則使用者可以建立並修改網路橋接器的設定。啟用此原則設定並不會從使用者的電腦移除現存的網路橋接器 | 電腦設定\系統管理範本\網路\網路連接\禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0013 | 網路\網路連線 | 禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | * 此項原則設定決定使用者是否可以安裝及設定網路橋接器 * 注意：此項設定與位置有關。只有當電腦連線到相同DNS網域網路，而且在這個連線上更新設定，才會套用此項設定。如果設定更新之後，電腦又連線到其他不同的DNS網域網路，此項設定將不會生效 * 網路橋接器可以讓使用者建立層級2MAC橋接器，啟用橋接器可以將兩個(含)以上的網路區段連在一起。這個連線會出現在「網路連線」資料夾中 * 如果停用或未設定此項原則設定，則使用者可以建立並修改網路橋接器的設定。啟用此原則設定並不會從使用者的電腦移除現存的網路橋接器 | 電腦設定\系統管理範本\網路\網路連線\禁止在您的DNS網域網路上安裝、設定及使用網路橋接 | 啟用 |
| 8 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0016 | 網路\Windows連線管理員 | 最小化網際網路或Windows網域的同時連線數目 | * 此項原則設定可防止電腦建立網際網路或Windows網域的多個同時連線。根據預設，當此項原則設定值是「未設定」時，預設為啟用 * 如果啟用此項原則設定，當電腦至少有一個使用的網際網路連線時，會封鎖新的網際網路自動連線嘗試。當電腦至少有一個使用中的Windows網域連線時，也會封鎖相同Windows網域的新自動連線。此項原則設定不會封鎖使用者對網際網路或Windows網域所執行的其他手動連線嘗試 * 在對網際網路或Windows網域有多個同時連線的情況下，當非慣用連線的網路流量低於特定閾值時，Windows會中斷非慣用連線。例如：當電腦使用Wi-Fi連線到網際網路，並以使用者外掛程式連線到乙太網路時，網路流量會透過較快的乙太網路連線路由，而減少Wi-Fi流量。Windows偵測到這種情況，然後以中斷Wi-Fi連線來回應 * 如果停用此項原則設定，則允許多個網際網路、Windows網域或兩者的同時連線 * 如果此項原則設定值是「未設定」，則會啟用預設原則設定。不過，這與使用群組原則啟用原則設定不同；當原則設定是「未啟用」時，使用者即可設定本機電腦上的原則設定。使用群組原則套用原則設定時，就無法在本機上設定。原則設定的值為「未設定」時，就不會建立新的自動連線嘗試，而且較不慣用的連線會被中斷 | 電腦設定\系統管理範本\網路\Windows連線管理員\最小化網際網路或Windows網域的同時連線數目 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0016 | 網路\Windows連線管理員 | 最小化網際網路或Windows網域的同時連線數目 | * 此項原則設定會決定電腦是否能對網際網路或Windows網域有多個連線。若允許多個連線，則會接著決定網路流量的路由方式 * 若此項原則設定設為「0=允許同時連線」，電腦就能對網際網路、Windows網域或兩者具有同時連線。網際網路流量可透過所有連線路由，包括行動數據連線和所有計量付費網路。這在此項原則設定原本處於「已停用」狀態 * 若此項原則設定設為「1=將同時連線最小化」，則會在電腦對慣用類型的網路至少有一個正在使用的網際網路連線時，封鎖所有新的自動化網際網路連線。此為慣用類型的順序(從最慣用至最不慣用排序)：乙太網路>WLAN>行動數據。乙太網路一律是慣用的連線類型，但使用者仍可手動連線至任何網路。這在此項原則設定中原本處於「已啟用」狀態 * 若此項原則設定設為「2=保持行動數據的連線」，則行為會與1相似。不過，若有行動數據連線可用，則會為需要行動數據連線的服務一律保持連線。當使用者連線至WLAN或乙太網路連線時，不會透過行動數據連線路由任何網際網路流量。此選項最早於Windows 10(1703版)提供使用 * 若此項原則設定設為「3=使用乙太網路時禁止Wi-Fi」，則行為會與2相似。不過，若存在乙太網路連線，Windows就不會允許使用者手動連線至WLAN。只有不存在乙太網路連線時才能連線(自動或手動)至WLAN | 電腦設定\系統管理範本\網路\Windows連線管理員\最小化網際網路或Windows網域的同時連線數目 | 啟用：3=使用乙太網路時禁止Wi-Fi |
| 9 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0018 | 網路\連結階層拓樸搜尋 | 開啟Mapper I/O(LLTDIO)驅動程式 | * 此項原則設定會變更Mapper I/O網路通訊協定驅動程式的操作行為 * LLTDIO允許電腦搜索其連線網路的拓撲。也允許電腦起始服務品質(Quality-of-Service)要求，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，使用者可以使用其他選項來微調選取項目可以選擇「允許在網域中操作」選項，以允許LLTDIO在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，使用者就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用LLTDIO的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜尋\開啟Mapper I/O(LLTDIO)驅動程式 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0018 | 網路\連結階層拓樸搜索 | 開啟Mapper I/O(LLTDIO)驅動程式 | * 此項原則設定會變更Mapper I/O網路通訊協定驅動程式的操作行為 * LLTDIO允許電腦搜索其連線網路的拓撲。也允許電腦起始服務品質(Quality-of-Service)要求，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，使用者可以使用其他選項來微調選取項目，可以選擇「允許在網域中操作」選項，以允許LLTDIO在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，使用者就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用LLTDIO的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟Mapper I/O(LLTDIO)驅動程式 | 停用 |
| 10 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0019 | 網路\連結階層拓樸搜尋 | 開啟Responder(RSPNDR)驅動程式 | * 此項原則設定決定是否變更Responder網路通訊協定驅動程式的操作行為 * Responder允許電腦加入「連結階層拓樸搜索」要求，以便能在網路上搜索並找到該電腦。也允許電腦加入服務品質(Quality-of-Service)活動，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，則可以使用其他選項來微調選取項目。若選擇「允許在網域中操作」選項，以允許Responder在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用Responder的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜尋\開啟Responder(RSPNDR)驅動程式 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0019 | 網路\連結階層拓樸搜索 | 開啟Responder(RSPNDR)驅動程式 | * 此項原則設定決定是否變更Responder網路通訊協定驅動程式的操作行為 * Responder允許電腦加入「連結階層拓樸搜索」要求，以便能在網路上搜索並找到該電腦。也允許電腦加入服務品質(Quality-of-Service)活動，例如頻寬估計和網路狀態分析 * 如果啟用此項原則設定，則可以使用其他選項來微調選取項目。若選擇「允許在網域中操作」選項，以允許Responder在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，就可以改為選擇「允許在公用網路中操作」與「禁止在私人網路中操作」 * 如果停用或未設定此項原則設定，將套用Responder的預設行為 | 電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟Responder(RSPNDR)驅動程式 | 停用 |
| 11 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0020 | 網路\Lanman工作站 | 啟用不安全的來賓登入 | * 此原則設定可決定SMB用戶端是否允許以不安全的來賓身分登入SMB伺服器 * 若啟用此原則設定或未設定此原則設定，SMB用戶端將允許不安全的來賓登入 * 若停用此原則設定，SMB用戶端將拒絕不安全的來賓登入 * 雖然在機關環境中不常見，做為檔案伺服器的消費性「網路連接儲存裝置」(NAS)設備經常使用不安全的來賓登入。Windows檔案伺服器需要驗證，而且預設不會使用不安全的來賓登入。因為不安全的來賓登入未經驗證，重要安全性功能(例如「SMB簽署」與「SMB加密」)會被停用。因此，允許不安全的來賓登入之用戶端容易遭受各種攔截式攻擊，進而導致資料遺失、資料損毀與暴露於惡意程式碼。此外，使用不安全的來賓登入方式寫入到檔案伺服器的所有資料可能可供網路上的任何人存取 | 電腦設定\系統管理範本\網路\Lanman工作站\啟用不安全的來賓登入 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0020 | 網路\Lanman工作站 | 啟用不安全的來賓登入 | * 此原則設定可決定SMB用戶端是否允許以不安全的來賓身分登入SMB伺服器 * 若啟用此原則設定或未設定此原則設定，SMB用戶端將允許不安全的來賓登入 * 若停用此原則設定，SMB用戶端將拒絕不安全的來賓登入 * 檔案伺服器使用不安全的來賓登入來允許共用資料夾的未經驗證存取，雖然在機關環境中不常見，做為檔案伺服器的消費性「網路連接儲存裝置」(NAS)設備經常使用不安全的來賓登入。Windows檔案伺服器需要驗證，而且預設不會使用不安全的來賓登入。因為不安全的來賓登入未經驗證，重要安全性功能(例如「SMB簽署」與「SMB加密」)會被停用。因此，允許不安全的來賓登入之用戶端容易遭受各種攔截式攻擊，進而導致資料遺失、資料損毀與暴露於惡意程式碼。此外，使用不安全的來賓登入方式寫入到檔案伺服器的所有資料可能可供網路上的任何人存取 | 電腦設定\系統管理範本\網路\Lanman工作站\啟用不安全的來賓登入 | 停用 |
| 12 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0025 | 網路\TCPIP設定值\IPv6轉換技術 | 設定Teredo狀態 | * 此項原則設定可讓使用者設定Teredo，它是在IPv4網際網路上提供單點傳播IPv6連線的位址指派與自動通道技術 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，可用下列其中一個設定來設定Teredo：   + 預設值：預設狀態是「用戶端」   + 停用：主機不提供Teredo介面   + 用戶端：只有當主機不是位在包含網域控制站的網路時，才提供Teredo介面   + 企業版用戶端：即使主機位在包含網域控制站的網路上，也會提供Teredo介面 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定Teredo狀態 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0025 | 網路\TCPIP設定值\IPv6轉換技術 | 設定Teredo狀態 | * 此項原則設定可讓使用者設定Teredo，它是在IPv4網際網路上提供單點傳播IPv6連線的位址指派與自動通道技術 * 如果停用或未設定此項原則設定，則使用本機主機設定 * 如果啟用此項原則設定，可用下列其中一個設定來設定Teredo：   + 預設狀態：預設狀態是「用戶端」   + 停用狀態：主機不提供Teredo介面   + 用戶端：只有當主機不是位在包含網域控制站的網路時，才提供Teredo介面   + 企業版用戶端：即使主機位在包含網域控制站的網路上，也會提供Teredo介面 | 電腦設定\系統管理範本\網路\TCPIP設定值\IPv6轉換技術\設定Teredo狀態 | 啟用 |
| 13 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0035 | 系統\登入 | 不要處理只執行一次清單 | * 此項原則設定會忽略自訂的執行一次清單 * 使用者可以建立一份系統在下次啟動時會自動啟動(但之後就不再自動啟動)的自訂額外程式與文件清單。這些程式會加入由系統啟動的程式與服務標準清單中 * 如果啟用此項原則設定，則系統會略過執行一次清單 * 如果停用或未設定此項原則設定，系統會執行只執行一次清單中的程式 * 此項原則設定會同時出現在「電腦設定」及「使用者設定」資料夾中。如果同時設定這兩個原則設定，則「電腦設定」中的原則設定將優先於「使用者設定」中的原則設定 * 注意：自訂的只執行一次清單存放在HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce的登錄中。另請參閱「不要處理舊版執行清單」原則設定 | 電腦設定\系統管理範本\系統\登入\不要處理只執行一次清單 | CCE-ID：CCE-44292-1 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0035 | 系統\登入 | 不要處理只執行一次清單 | * 此項原則設定會忽略自訂的執行一次清單 * 使用者可以建立一份系統在下次啟動時會自動啟動(但之後就不再自動啟動)的自訂額外程式與文件清單。這些程式會加入由系統啟動的程式與服務標準清單中 * 如果啟用此項原則設定，則系統會略過執行一次清單 * 如果停用或未設定此項原則設定，系統會執行只執行一次清單中的程式 * 此項原則設定會同時出現在「電腦設定」與「使用者設定」資料夾中。如果同時設定這兩個原則設定，則「電腦設定」中的原則設定將優先於「使用者設定」中的原則設定 * 注意：自訂的只執行一次清單存放在HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce的登錄中 | 電腦設定\系統管理範本\系統\登入\不要處理只執行一次清單 | CCE-ID：CCE-44292-1 |
| 14 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0044 | 系統\遠端協助 | 開啟工作階段記錄 | * 此項原則設定可讓使用者開啟或關閉記錄。記錄檔位於使用者之「遠端協助」下的「文件」資料夾中 * 如果啟用此項原則設定，就會產生記錄檔 * 如果停用此項原則設定，就不會產生記錄檔 * 如果未設定此項原則設定，就會使用以應用程式為基礎的設定 | 電腦設定\系統管理範本\系統\遠端協助\開啟工作階段紀錄 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0044 | 系統\遠端協助 | 開啟工作階段記錄 | * 此項原則設定可讓使用者開啟或關閉記錄。記錄檔位於使用者之「遠端協助」下的「文件」資料夾中 * 如果啟用此項原則設定，就會產生記錄檔 * 如果停用此項原則設定，就不會產生記錄檔 * 如果未設定此項原則設定，就會使用以應用程式為基礎的設定 | 電腦設定\系統管理範本\系統\遠端協助\開啟工作階段記錄 | 啟用 |
| 15 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0049 | 系統\裝置安裝 | 指定裝置驅動程式來源位置的搜尋順序 | * 此項原則設定決定是否指定Windows搜尋裝置驅動程式的來源位置時的搜尋順序 * 如果啟用此項原則設定，使用者可以選擇讓Windows先搜尋WindowsUpdate、後搜尋WindowsUpdate，或不搜尋WindowsUpdate * 如果停用或未設定此項原則設定，則Administrators群組的成員可以決定Windows會依什麼順序搜尋裝置驅動程式的來源位置 | 電腦設定\系統管理範本\系統\裝置安裝\指定裝置驅動程式來源位置的搜尋順序 | 啟用，不搜尋Windows Update |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0049 | 系統\裝置安裝 | 指定裝置驅動程式來源位置的搜尋順序 | * 此項原則設定決定是否指定Windows搜尋裝置驅動程式的來源位置時的搜尋順序 * 如果啟用此項原則設定，使用者可以選擇Windows在WindowsUpdate搜尋驅動程式為無條件搜尋、僅需要時搜尋或不搜尋 * 如果停用或未設定此項原則設定，則Administrators群組的成員可以決定Windows會依什麼順序搜尋裝置驅動程式的來源位置 | 電腦設定\系統管理範本\系統\裝置安裝\指定裝置驅動程式來源位置的搜尋順序 | 啟用，不搜尋Windows Update |
| 16 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0054 | 系統\Windows時間服務\時間提供者 | 設定Windows NTP用戶端 | * 此項原則設定決定是否指定用於控制Windows NTP用戶端的參數組   + NtpServer：NTP時間來源的網域名稱系統(DNS)名稱或IP位址。這個值的格式為「dnsName，flags」，其中flags是該主機之旗標的十六進位位元遮罩   + Type：這個值用於控制W32time使用的驗證方式。預設值是NT5DS   + CrossSiteSyncFlags：這個值以位元遮罩形式表示，用於控制W32time如何選擇其站台以外的時間來源。可能的值為0、1及2  1. 這個值若設為0(無)，表示時間用戶端不應嘗試與站台外進行時間同步 2. 這個值若設為1(PdcOnly)，表示當用戶端必須與其站台以外的夥伴進行時間同步時，只有在其他網域做為網域主控站(PDC)模擬器操作主機的電腦可做為同步夥伴使用 3. 這個值若設為2(全部)，則表示可以使用任何同步夥伴。如果未設定NT5DS值，就會忽略這個值。預設值是十進位2(十六進位0x02)    * ResolvePeerBackoffMinutes：這個值(以分鐘表示)用於控制W32time在前次嘗試失敗後，於嘗試解析DNS名稱前等候的時間長度。預設值是15分鐘    * ResolvePeerBackoffMaxTimes：這個值用於控制W32time在重新啟動探索處理程序之前，嘗試解析DNS名稱的次數。DNS名稱解析每失敗一次，下次嘗試之前等候的時間長度都將是前次時間長度的兩倍。預設值是7次嘗試    * SpecialPollInterval：這個NTP用戶端值以秒鐘表示，用於控制當手動設定的時間來源設定為使用特殊輪詢間隔時，該時間來源的輪詢頻率。如果NTPServer設定已啟用SpecialInterval旗標，用戶端會使用設定為SpecialPollInterval的值(而不是MinPollInterval和MaxPollInterval值)來判定輪詢時間來源的頻率。預設值是1024秒    * EventLogFlags：這個值是位元遮罩，用於控制可記錄到事件檢視器中系統記錄檔的事件。這個值若設為0x1，表示每次偵測到時間跳躍時，W32time都會建立事件。這個值若設為0x2，表示每次發生時間來源變更時，W32time都會建立事件。因為它是位元遮罩值，所以設定0x3(0x1加上0x2)表示時間跳躍和時間來源變更都會留下紀錄 | 電腦設定\系統管理範本\系統\Windows時間服務\時間提供者\設定Windows NTP用戶端 | 啟用， NTP Server：time.nist.gov 類型： NT5DS CrossSiteSyncFlags：2 ResolvePeerBackoffMinutes：15 ResolvePeerBackoffMaxTimes：7 SpecialPollInterval：3600 EventLogFlags：0 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0054 | 系統\Windows時間服務\時間提供者 | 設定Windows NTP用戶端 | * 此項原則設定決定是否指定用於控制Windows NTP用戶端的參數組 * 如果啟用此項原則設定，可以指定Windows NTP用戶端的下列參數 * 如果停用或未設定此項原則設定，Windows NTP用戶端會使用下列每個參數的預設值   + NtpServer：NTP時間來源的網域名稱系統(DNS)名稱或IP位址。這個值的格式為「dnsName，flags」，其中flags是該主機之旗標的十六進位位元遮罩，預設值是time.windows.com,0x09   + Type：這個值用於控制W32time使用的驗證方式。預設值是NT5DS   + CrossSiteSyncFlags：這個值以位元遮罩形式表示，用於控制W32time如何選擇其站台以外的時間來源。可能的值為0、1及2  1. 這個值若設為0(無)，表示時間用戶端不應嘗試與站台外進行時間同步 2. 這個值若設為1(PdcOnly)，表示當用戶端必須與其站台以外的夥伴進行時間同步時，只有在其他網域做為網域主控站(PDC)模擬器操作主機的電腦可做為同步夥伴使用 3. 這個值若設為2(全部)，則表示可以使用任何同步夥伴。如果未設定NT5DS值，就會忽略這個值。預設值是十進位2(十六進位0x02)    * ResolvePeerBackoffMinutes：這個值(以分鐘表示)用於控制W32time在前次嘗試失敗後，於嘗試解析DNS名稱前等候的時間長度。預設值是15分鐘    * ResolvePeerBackoffMaxTimes：這個值用於控制W32time在重新啟動探索處理程序之前，嘗試解析DNS名稱的次數。DNS名稱解析每失敗一次，下次嘗試之前等候的時間長度都將是前次時間長度的兩倍。預設值是7次嘗試    * SpecialPollInterval：這個NTP用戶端值以秒鐘表示，用於控制當手動設定的時間來源設定為使用特殊輪詢間隔時，該時間來源的輪詢頻率。如果NTPServer設定已啟用SpecialInterval旗標，用戶端會使用設定為SpecialPollInterval的值(而不是MinPollInterval和MaxPollInterval值)來判定輪詢時間來源的頻率。預設值是1024秒    * EventLogFlags：這個值是位元遮罩，用於控制可記錄到事件檢視器中系統記錄檔的事件。這個值若設為0x1，表示每次偵測到時間跳躍時，W32time都會建立事件。這個值若設為0x2，表示每次發生時間來源變更時，W32time都會建立事件。因為它是位元遮罩值，所以設定0x3(0x1加上0x2)表示時間跳躍和時間來源變更都會留下紀錄 | 電腦設定\系統管理範本\系統\Windows時間服務\時間提供者\設定Windows NTP用戶端 | 啟用， NTP Server：time.nist.gov 類型： NT5DS CrossSiteSyncFlags：2 ResolvePeerBackoffMinutes：15 ResolvePeerBackoffMaxTimes：7 SpecialPollInterval：3600 EventLogFlags：0 |
| 17 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0063 | 網際網路通訊管理\網際網路通訊設定 | 關閉手寫辨識錯誤報告 | * 此項原則設定決定是否關閉手寫辨識錯誤報告工具。使用者可以使用手寫辨識錯誤報告工具來報告在「TabletPC輸入面板」中發生的錯誤。此工具可產生錯誤報告，並透過安全連線將報告傳輸至Microsoft * Microsoft將使用這些錯誤報告來改善未來Windows版本中的手寫辨識功能 * 如果啟用此項原則，使用者將無法啟動手寫辨識錯誤報告工具，或是將錯誤報告傳送給Microsoft * 如果啟用此項原則，則TabletPC使用者可以將手寫辨識錯誤報告給Microsoft * 如果未設定此項原則，則TabletPC使用者可以將手寫辨識錯誤報告給Microsoft | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉手寫辨識錯誤報告 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0063 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉手寫辨識錯誤報告 | * 此項原則設定決定是否關閉手寫辨識錯誤報告工具。使用者可以使用手寫辨識錯誤報告工具來報告在「TabletPC輸入面板」中發生的錯誤。此工具可產生錯誤報告，並透過安全連線將報告傳輸至Microsoft，Microsoft將使用這些錯誤報告來改善未來Windows版本中的手寫辨識功能 * 如果啟用此項原則，使用者將無法啟動手寫辨識錯誤報告工具，或是將錯誤報告傳送給Microsoft * 如果停用或未設定此項原則，則TabletPC使用者可以將手寫辨識錯誤報告給Microsoft | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉手寫辨識錯誤報告 | 啟用 |
| 18 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0067 | 網際網路通訊管理\網際網路通訊設定 | 關閉Windows錯誤報告 | * 此項原則設定控制是否向Microsoft報告錯誤 * 錯誤報告是用來報告系統或應用程式失敗或停止回應的相關資訊，並用來改進產品的品質 * 如果啟用此項原則設定，使用者將無法報告錯誤 * 如果停用或未設定此項原則設定，可以透過網際網路或機關的檔案共用向Microsoft報告錯誤。此項原則設定會覆寫任何從控制台對報告錯誤所做的使用者設定 * 此外，也可以參閱「電腦設定/系統管理範本/Windows元件/Windows錯誤報告」中的「設定錯誤報告」、「顯示錯誤通知」和「停用Windows錯誤報告」原則設定 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows錯誤報告 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0067 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉Windows錯誤報告 | * 此項原則設定控制是否向Microsoft報告錯誤 * 錯誤報告是用來報告系統或應用程式失敗或停止回應的相關資訊，並用來改進產品的品質 * 如果啟用此項原則設定，使用者將無法報告錯誤 * 如果停用或未設定此項原則設定，可以透過網際網路或機關的檔案共用向Microsoft報告錯誤。此項原則設定會覆寫任何從控制台對報告錯誤所做的使用者設定 * 此外，也可以參閱「電腦設定/系統管理範本/Windows元件/Windows錯誤報告」中的「設定錯誤報告」、「顯示錯誤通知」和「停用Windows錯誤報告」原則設定 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows錯誤報告 | 啟用 |
| 19 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0070 | 進階稽核原則設定 | 稽核原則：帳戶登入：稽核驗證認證 | * 此項原則設定可讓使用者稽核因使用者帳戶登入認證的驗證測試而產生的事件 * 只有在授權可以使用那些認證的電腦上，才會發生這個子類別中的事件。如果是網域帳戶，則網域控制站具有授權。如果是本機帳戶，則本機電腦具有授權 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\稽核原則：帳戶登入：稽核驗證認證 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0070 | 進階稽核原則設定 | 稽核驗證認證 | * 此項原則設定可讓使用者稽核因使用者帳戶登入認證的驗證測試而產生的事件 * 只有在授權可以使用那些認證的電腦上，才會發生這個子類別中的事件。如果是網域帳戶，則網域控制站具有授權。如果是本機帳戶，則本機電腦具有授權 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶登入\稽核驗證認證 | 成功與失敗 |
| 20 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0071 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核電腦帳戶管理 | * 此項原則設定可稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 * 如果設定此項原則，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則，則不會在電腦帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核原則：帳戶管理：稽核電腦帳戶管理 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0071 | 進階稽核原則設定 | 稽核電腦帳戶管理 | * 此項原則設定可稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 * 如果設定此項原則，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則，則不會在電腦帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核電腦帳戶管理 | 成功 |
| 21 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0072 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核其他帳戶管理事件 | * 此項原則設定可讓使用者稽核因這個類別未涵蓋的其他使用者帳戶變更而產生的事件，例如：   + 已存取使用者帳戶的密碼雜湊。這一般是在Active Directory管理工具密碼移轉期間發生   + 已呼叫密碼原則檢查API。在惡意應用程式測試原則以減少密碼字典攻擊期間的嘗試次數時，呼叫這個功能會是一種攻擊 * 下列群組原則路徑下的預設網域群組原則變更：   + 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則   + 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則 * 注意：套用原則設定時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核其他帳戶管理事件 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0072 | 進階稽核原則設定 | 稽核其他帳戶管理事件 | * 此項原則設定可讓使用者稽核因這個類別未涵蓋的其他使用者帳戶變更而產生的事件，例如： * 已存取使用者帳戶的密碼雜湊。這一般是在Active Directory管理工具密碼移轉期間發生 * 已呼叫密碼原則檢查API。在惡意應用程式測試原則以減少密碼字典攻擊期間的嘗試次數時，呼叫這個功能會是一種攻擊 * 下列群組原則路徑下的預設網域群組原則變更： * 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則 * 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則 * 注意：套用原則設定時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核其他帳戶管理事件 | 成功與失敗 |
| 22 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0073 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核安全性群組管理 | * 此項原則設定可稽核因安全性群組變更而產生的事件，例如： * 建立、變更或刪除安全性群組 * 在安全性群組中新增或移除成員 * 變更群組類型 * 如果設定此項原則設定，則會在嘗試變更安全性群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在安全性群組變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核安全性群組管理 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0073 | 進階稽核原則設定 | 稽核安全性群組管理 | * 此項原則設定可稽核因安全性群組變更而產生的事件，例如： * 建立、變更或刪除安全性群組 * 在安全性群組中新增或移除成員 * 變更群組類型 * 如果設定此項原則設定，則會在嘗試變更安全性群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在安全性群組變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核安全性群組管理 | 成功與失敗 |
| 23 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0074 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核使用者帳戶管理 | * 此項原則設定可稽核使用者帳戶的變更。包含下列事件： * 建立、變更、刪除、重新命名、停用、啟用、鎖定或解除鎖定使用者帳戶 * 設定或變更使用者帳戶的密碼 * 將安全性識別碼(SID)新增到使用者帳戶的SID歷程記錄 * 設定目錄服務還原模式密碼 * 變更管理使用者帳戶的權限 * 備份或還原認證管理員認證 * 如果設定此項原則設定，則會在嘗試變更使用者帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在使用者帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核使用者帳戶管理 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0074 | 進階稽核原則設定 | 稽核使用者帳戶管理 | * 此項原則設定可稽核使用者帳戶的變更。包含下列事件： * 建立、變更、刪除、重新命名、停用、啟用、鎖定或解除鎖定使用者帳戶 * 設定或變更使用者帳戶的密碼 * 將安全性識別碼(SID)新增到使用者帳戶的SID歷程記錄 * 設定目錄服務還原模式密碼 * 變更管理使用者帳戶的權限 * 備份或還原認證管理員認證 * 如果設定此項原則設定，則會在嘗試變更使用者帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在使用者帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核使用者帳戶管理 | 成功與失敗 |
| 24 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0075 | 進階稽核原則設定 | 稽核原則：詳細追蹤：稽核建立處理程序 | * 此項原則設定可稽核建立或啟動處理程序時產生的事件，也會稽核建立處理程序的應用程式或使用者名稱 * 如果設定此項原則設定，則會在建立處理程序時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在建立處理程序時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核原則：詳細追蹤：稽核建立處理程序 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0075 | 進階稽核原則設定 | 稽核建立處理程序 | * 此項原則設定可稽核建立或啟動處理程序時產生的事件，也會稽核建立處理程序的應用程式或使用者名稱 * 如果設定此項原則設定，則會在建立處理程序時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在建立處理程序時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核建立處理程序 | 成功 |
| 25 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0076 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核帳戶鎖定 | * 此項原則設定可稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 * 若設定此原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 * 登入事件對於了解使用者活動以及偵測潛在的攻擊是十分重要的 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核帳戶鎖定 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0076 | 進階稽核原則設定 | 稽核帳戶鎖定 | * 此項原則設定可稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 * 若設定此原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 * 登入事件對於了解使用者活動以及偵測潛在的攻擊是十分重要的 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核帳戶鎖定 | 成功與失敗 |
| 26 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0077 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核登出 | * 此項原則設定可稽核因關閉登入工作階段而產生的事件。這些事件發生於被存取的電腦上。如果是互動式登出，則會在使用者帳戶登入的電腦上產生安全性稽核事件 * 如果設定此項原則設定，則會在關閉登入工作階段時產生稽核事件。成功稽核會記錄成功關閉工作階段嘗試，而失敗稽核則會記錄失敗關閉工作階段嘗試 * 如果未設定此項原則設定，則不會在關閉登入工作階段時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核登出 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0077 | 進階稽核原則設定 | 稽核登出 | * 此項原則設定可稽核因關閉登入工作階段而產生的事件。這些事件發生於被存取的電腦上。如果是互動式登出，則會在使用者帳戶登入的電腦上產生安全性稽核事件 * 如果設定此項原則設定，則會在關閉登入工作階段時產生稽核事件。成功稽核會記錄成功關閉工作階段嘗試，而失敗稽核則會記錄失敗關閉工作階段嘗試 * 如果未設定此項原則設定，則不會在關閉登入工作階段時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核登出 | 成功 |
| 27 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0078 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核登入 | * 此項原則設定可讓使用者稽核因電腦上的使用者帳戶登入嘗試而產生的事件 * 這個子類別中的事件是與建立登入工作階段有關，而且發生在被存取的電腦上。如果是互動式登入，則會在使用者帳戶登入的電腦上產生安全性稽核事件。如果是網路登入(如存取網路上的共用資料夾)，則會在裝載資源的電腦上產生安全性稽核事件。包含下列事件： * 成功登入嘗試 * 失敗登入嘗試 * 使用明確認證的登入嘗試。處理程序嘗試明確指定該帳戶的認證來登入帳戶時，會產生這個事件。這最常發生於批次登入設定(如排定的工作或使用RUNAS命令時) * 已篩選安全性識別碼(SID)且不允許其登入 * 數量：用戶端電腦上是「低」。網域控制站或網路伺服器上是「中」 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核登入 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0078 | 進階稽核原則設定 | 稽核登入 | * 此項原則設定可讓使用者稽核因電腦上的使用者帳戶登入嘗試而產生的事件 * 這個子類別中的事件是與建立登入工作階段有關，而且發生在被存取的電腦上。如果是互動式登入，則會在使用者帳戶登入的電腦上產生安全性稽核事件。如果是網路登入(如存取網路上的共用資料夾)，則會在裝載資源的電腦上產生安全性稽核事件。包含下列事件： * 成功登入嘗試 * 失敗登入嘗試 * 使用明確認證的登入嘗試。處理程序嘗試明確指定該帳戶的認證來登入帳戶時，會產生這個事件。這最常發生於批次登入設定(如排定的工作或使用RUNAS命令時) * 已篩選安全性識別碼(SID)且不允許其登入 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核登入 | 成功與失敗 |
| 28 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0079 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核特殊登入 | * 此項原則設定可稽核因特殊登入而產生的事件，例如： * 使用特殊登入，這是具有管理員同等權限而且可以用來將處理程序提高為較高等級的登入 * 特殊群組成員的登入。特殊群組可讓使用者稽核特定群組成員登入網路時產生的事件 * 可在登錄中設定群組安全性識別碼(SID)清單。如果上述任一SID在登入期間被新增至權杖，而且子類別已啟用，則會記錄事件。如需這個功能的詳細資訊，請參閱Microsoft知識庫文章947223(http：//go.microsoft.com/fwlink/?LinkId=121697) | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核特殊登入 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0079 | 進階稽核原則設定 | 稽核特殊登入 | * 此項原則設定可稽核因特殊登入而產生的事件，例如： * 使用特殊登入，這是具有管理員同等權限而且可以用來將處理程序提高為較高等級的登入 * 特殊群組成員的登入。特殊群組可讓使用者稽核特定群組成員登入網路時產生的事件 * 可在登錄中設定群組安全性識別碼(SID)清單。如果上述任一SID在登入期間被新增至權杖，而且子類別已啟用，則會記錄事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核特殊登入 | 成功 |
| 29 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0080 | 進階稽核原則設定 | 稽核原則：物件存取：稽核抽取式存放裝置 | * 此項原則設定可稽核存取抽取式存放裝置上之檔案系統物件的使用者嘗試。安全性稽核事件只會針對所有要求之存取類型的所有物件產生 * 如果設定此原則設定，每當有帳戶存取抽取式存放裝置上的檔案系統物件時，就會產生稽核事件。成功稽核會記錄成功的嘗試，失敗稽核會記錄失敗的嘗試 * 如果未設定此原則設定，當有帳戶存取抽取式存放裝置上的檔案系統物件時，就不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核原則：物件存取：稽核抽取式存放裝置 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0080 | 進階稽核原則設定 | 稽核抽取式存放裝置 | * 此項原則設定可稽核存取抽取式存放裝置上之檔案系統物件的使用者嘗試。安全性稽核事件只會針對所有要求之存取類型的所有物件產生 * 如果設定此原則設定，每當有帳戶存取抽取式存放裝置上的檔案系統物件時，就會產生稽核事件。成功稽核會記錄成功的嘗試，失敗稽核會記錄失敗的嘗試 * 如果未設定此原則設定，當有帳戶存取抽取式存放裝置上的檔案系統物件時，就不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核抽取式存放裝置 | 成功 |
| 30 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0081 | 進階稽核原則設定 | 稽核原則：原則變更：稽核「稽核原則變」更」 | * 此項原則設定可稽核安全性稽核原則設定變更，例如： * 稽核原則物件上的設定權限及稽核設定 * 系統稽核原則的變更 * 安全性事件來源的註冊 * 解除安全性事件來源的註冊 * 每個使用者稽核設定的變更 * CrashOnAuditFail值的變更 * 檔案系統或登錄物件上的系統存取控制清單變更 * 特殊群組清單的變更 * 注意：物件的SACL變更而且已啟用原則變更類別時，會進行系統存取控制清單(SACL)變更稽核。啟用物件存取稽核且設定物件的SACL以稽核DACL/擁有者變更時，會稽核判別存取控制清單(DACL)及擁有權變更 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核原則：原則變更：稽核「稽核原則變更」 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0081 | 進階稽核原則設定 | 稽核「稽核原則變更」 | * 此項原則設定可稽核安全性稽核原則設定變更，例如： * 稽核原則物件上的設定權限及稽核設定 * 系統稽核原則的變更 * 安全性事件來源的註冊 * 解除安全性事件來源的註冊 * 每個使用者稽核設定的變更 * CrashOnAuditFail值的變更 * 檔案系統或登錄物件上的系統存取控制清單變更 * 特殊群組清單的變更 * 注意：物件的SACL變更而且已啟用原則變更類別時，會進行系統存取控制清單(SACL)變更稽核。啟用物件存取稽核且設定物件的SACL以稽核DACL/擁有者變更時，會稽核判別存取控制清單(DACL)及擁有權變更 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核「稽核原則變更」 | 成功與失敗 |
| 31 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0082 | 進階稽核原則設定 | 稽核原則：原則變更：稽核驗證原則變更 | * 此項原則設定可稽核因驗證原則變更而產生的事件，例如： * 建立樹系及網域信任 * 修改樹系及網域信任 * 移除樹系及網域信任 * 變更下列位置下的Kerberos原則：電腦設定\Windows設定\安全性設定\帳戶原則\Kerberos原則 * 將下列任何使用者權限授與使用者或群組： * 從網路存取這台電腦 * 允許本機登入 * 允許透過終端機服務登入 * 以批次工作登入 * 以服務方式登入 * 命名空間衝突。例如，新信任的名稱與現有命名空間名稱相同時 * 如果設定此項原則設定，則會在嘗試變更驗證原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更驗證原則時產生稽核事件 * 注意：套用群組原則時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核原則：原則變更：稽核驗證原則變更 | 成功 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0082 | 進階稽核原則設定 | 稽核驗證原則變更 | * 此項原則設定可稽核因驗證原則變更而產生的事件，例如： * 建立樹系及網域信任 * 修改樹系及網域信任 * 移除樹系及網域信任 * 變更下列位置下的Kerberos原則：電腦設定\Windows設定\安全性設定\帳戶原則\Kerberos原則 * 將下列任何使用者權限授與使用者或群組： * 從網路存取這台電腦 * 允許本機登入 * 允許透過終端機服務登入 * 以批次工作登入 * 以服務方式登入 * 命名空間衝突。例如，新信任的名稱與現有命名空間名稱相同時 * 如果設定此項原則設定，則會在嘗試變更驗證原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更驗證原則時產生稽核事件 * 注意：套用群組原則時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核驗證原則變更 | 成功 |
| 32 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0083 | 進階稽核原則設定 | 稽核原則：特殊權限使用：稽核機密特殊權限使用 | * 此項原則設定可稽核使用機密特殊權限(使用者權限)時產生的事件，例如： * 呼叫特許服務 * 呼叫下列其中一種權限：  1. 當成作業系統的一部分 2. 備份檔案及目錄 3. 建立權杖物件 4. 偵錯程式 5. 讓電腦及使用者帳戶受信賴，以進行委派 6. 產生安全性稽核 7. 在驗證後模擬用戶端 8. 載入及解除載入裝置驅動程式 9. 管理稽核及安全性記錄檔 10. 修改韌體環境值 11. 取代處理程序等級權杖 12. 還原檔案及目錄 13. 取得檔案或其他物件的擁有權  * 如果設定此項原則設定，則會在進行機密特殊權限要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 * 如果未設定此項原則設定，則不會進行機密特殊權限要求時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\特殊權限使用\稽核原則：特殊權限使用：稽核機密特殊權限使用 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0083 | 進階稽核原則設定 | 稽核機密特殊權限使用 | * 此項原則設定可稽核使用機密特殊權限(使用者權限)時產生的事件，例如： * 呼叫特許服務 * 呼叫下列其中一種權限：  1. 當成作業系統的一部分 2. 備份檔案及目錄 3. 建立權杖物件 4. 偵錯程式 5. 讓電腦及使用者帳戶受信賴，以進行委派 6. 產生安全性稽核 7. 在驗證後模擬用戶端 8. 載入及解除載入裝置驅動程式 9. 管理稽核及安全性記錄檔 10. 修改韌體環境值 11. 取代處理程序等級權杖 12. 還原檔案及目錄 13. 取得檔案或其他物件的擁有權  * 如果設定此項原則設定，則會在進行機密特殊權限要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 * 如果未設定此項原則設定，則不會進行機密特殊權限要求時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\特殊權限使用\稽核機密特殊權限使用 | 成功與失敗 |
| 33 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0084 | 進階稽核原則設定 | 稽核原則：系統：稽核IPsec驅動程式 | * 此項原則設定可稽核因IPsec篩選器驅動程式而產生的事件，例如： * IPsec服務的啟動及關閉 * 因完整性檢查失敗而丟棄的網路封包 * 因重新執行檢查失敗而丟棄的網路封包 * 因格式為純文字而丟棄的網路封包 * 接收到具有不正確安全性參數索引(SPI)的網路封包。這可能表示網路卡未正確運作，或需要更新驅動程式 * 無法處理IPsec篩選器 * 如果設定此項原則設定，則會在IPsec篩選器驅動程式操作上產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在IPsec篩選器驅動程式操作上產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核IPsec驅動程式 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0084 | 進階稽核原則設定 | 稽核IPsec驅動程式 | * 此項原則設定可稽核因IPsec篩選器驅動程式而產生的事件，例如： * IPsec服務的啟動及關閉 * 因完整性檢查失敗而丟棄的網路封包 * 因重新執行檢查失敗而丟棄的網路封包 * 因格式為純文字而丟棄的網路封包 * 接收到具有不正確安全性參數索引(SPI)的網路封包。這可能表示網路卡未正確運作，或需要更新驅動程式 * 無法處理IPsec篩選器 * 如果設定此項原則設定，則會在IPsec篩選器驅動程式操作上產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在IPsec篩選器驅動程式操作上產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核IPsec驅動程式 | 成功與失敗 |
| 34 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0085 | 進階稽核原則設定 | 稽核原則：系統：稽核其他系統事件 | * 此項原則設定可稽核下列任一事件： * Windows防火牆服務及驅動程式的啟動及關閉 * Windows防火牆服務的安全性原則處理 * 加密編譯金鑰檔案及移轉操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\稽核原則: 系統: 稽核其他系統事件 | 失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0085 | 進階稽核原則設定 | 稽核其他系統事件 | * 此項原則設定可稽核下列任一事件： * Windows防火牆服務及驅動程式的啟動及關閉 * Windows防火牆服務的安全性原則處理 * 加密編譯金鑰檔案與移轉操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核其他系統事件 | 失敗 |
| 35 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0086 | 進階稽核原則設定 | 稽核原則：系統：稽核安全性狀態變更 | * 此項原則設定可稽核因電腦安全性狀態變更而產生的事件，例如下列事件： * 電腦的啟動及關閉 * 系統時間的變更 * 從CrashOnAuditFail復原系統，這是在安全性事件記錄檔已滿且設定CrashOnAuditFail登錄項目時於系統重新啟動之後記錄 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核安全性狀態變更 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0086 | 進階稽核原則設定 | 稽核安全性狀態變更 | * 此項原則設定可稽核因電腦安全性狀態變更而產生的事件，例如下列事件： * 電腦的啟動及關閉 * 系統時間的變更 * 從CrashOnAuditFail復原系統，這是在安全性事件記錄檔已滿且設定CrashOnAuditFail登錄項目時於系統重新啟動之後記錄 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核安全性狀態變更 | 成功與失敗 |
| 36 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0087 | 進階稽核原則設定 | 稽核原則：系統：稽核安全性系統延伸 | * 此項原則設定可稽核與安全性系統延伸或服務相關的事件，例如： * 載入安全性系統延伸(如驗證、通知或安全性封裝)，並向本機安全性授權(LSA)進行註冊。它是用來驗證登入嘗試、提交登入要求，以及任何帳戶或密碼變更，Kerberos及NTLM是安全性系統延伸的範例 * 安裝服務，並向服務控制管理員進行註冊。稽核記錄包含服務名稱、二進位、類型、啟動類型及服務帳戶的相關資訊 * 如果設定此項原則設定，則會在嘗試載入安全性系統延伸時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在嘗試載入安全性系統延伸時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核安全性系統延伸 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0087 | 進階稽核原則設定 | 稽核安全性系統延伸 | * 此項原則設定可稽核與安全性系統延伸或服務相關的事件，例如： * 載入安全性系統延伸(如驗證、通知或安全性封裝)，並向本機安全性授權(LSA)進行註冊。它是用來驗證登入嘗試、提交登入要求，以及任何帳戶或密碼變更，Kerberos及NTLM是安全性系統延伸的範例 * 安裝服務，並向服務控制管理員進行註冊。稽核記錄包含服務名稱、二進位、類型、啟動類型及服務帳戶的相關資訊 * 如果設定此項原則設定，則會在嘗試載入安全性系統延伸時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在嘗試載入安全性系統延伸時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核安全性系統延伸 | 成功與失敗 |
| 37 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0088 | 進階稽核原則設定 | 稽核原則：系統：稽核系統完整性 | * 此項原則設定可稽核會破壞安全性子系統完整性的事件，例如： * 因稽核系統發生問題而無法寫入事件記錄檔的事件 * 使用本機程序呼叫(LPC)連接埠的處理程序，而此連接埠在透過與用戶端位址空間之間的回覆、讀取或寫入來嘗試模擬用戶端的過程中無效 * 偵測到危害系統完整性的遠端程序呼叫(RPC) * 偵測到程式碼完整性判斷為無效之可執行檔的雜湊值 * 危害系統完整性的加密編譯操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核系統完整性 | 成功與失敗 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0088 | 進階稽核原則設定 | 稽核系統完整性 | * 此項原則設定可稽核會破壞安全性子系統完整性的事件，例如： * 因稽核系統發生問題而無法寫入事件記錄檔的事件 * 使用本機程序呼叫(LPC)連接埠的處理程序，而此連接埠在透過與用戶端位址空間之間的回覆、讀取或寫入來嘗試模擬用戶端的過程中無效 * 偵測到危害系統完整性的遠端程序呼叫(RPC) * 偵測到程式碼完整性判斷為無效之可執行檔的雜湊值 * 危害系統完整性的加密編譯操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核系統完整性 | 成功與失敗 |
| 38 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0090 | 安全性選項\帳戶 | 帳戶：封鎖Microsoft帳戶 | * 此原則設定可防止使用者在此電腦上新增Microsoft帳戶 * 若選取「使用者無法新增Microsoft帳戶」選項，使用者將無法在此電腦上建立新的Microsoft帳戶、從本機帳戶切換為Microsoft帳戶，或將網域帳戶關聯到Microsoft帳戶。若使用者必須在機關中限制Microsoft帳戶的使用，此為偏好的選項 * 若選取「使用者無法新增Microsoft帳戶或以Microsoft帳戶登入」選項，現有的Microsoft帳戶使用者將無法登入Windows。選取此選項可能會使此電腦的現有系統管理員無法登入並管理系統 * 若停用或不設定此原則(建議做法)，使用者將可以在Windows使用Microsoft帳戶 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：封鎖Microsoft帳戶 | 啟用，使用者無法新增Microsoft帳戶或以Microsoft帳戶登入 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0090 | 安全性選項\帳戶 | 帳戶：封鎖Microsoft帳戶 | * 此原則設定可防止透過「設定」應用程式為Microsoft服務和某些背景服務的單一登入(SSO)身分驗證新增Microsoft帳戶，或者使用 Microsoft帳戶對其他應用程式或服務進行單一登入 * 如果啟用此設定，將有2個選項： * 若選取「使用者無法新增Microsoft帳戶」選項，代表現有的已連線帳戶仍可以登入此裝置(並出現在登入螢幕上)。不過使用者無法使用「設定」應用程式新增新的連線帳戶(或將本地帳戶連線至Microsoft帳戶) * 若選取「使用者無法新增Microsoft帳戶或以Microsoft帳戶登入」選項，代表使用者無法新增新的連線帳戶(或將本地帳戶連線至Microsoft帳戶)，或是透過設定使用現有的連線帳戶 * 此設定並不影響為應用程式驗證新增Microsoft帳戶。例如，如果此設定啟用，使用者仍然可以提供一個Microsoft帳戶，透過Mail等應用程式進行驗證，但使用者無法使用Microsoft帳戶為其他應用程式或服務進行單一登入驗證(換句話說，使用者將會收到其他應用程式或服務的驗證提示) | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：封鎖Microsoft帳戶 | 啟用，使用者無法新增Microsoft帳戶或以Microsoft帳戶登入 |
| 39 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0107 | 安全性選項\網域成員 | 網域成員：最長電腦帳戶密碼有效期 | 此項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：最長電腦帳戶密碼有效期 | 30天 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0107 | 安全性選項\網域成員 | 網域成員：最長電腦帳戶密碼有效期 | 此項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網域成員：最長電腦帳戶密碼有效期 | 30天以下，但須大於0天 |
| 40 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0112 | 安全性選項\互動式登入 | 互動式登入：電腦未使用時間限制 | Windows會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時執行螢幕保護裝置並鎖定該工作階段 | 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：電腦未使用時間限制 | 900秒 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0112 | 安全性選項\互動式登入 | 互動式登入：電腦未使用時間限制 | Windows會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時執行螢幕保護裝置並鎖定該工作階段 | 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：電腦未使用時間限制 | 900秒以下，但須大於0秒 |
| 41 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0113 | 安全性選項\互動式登入 | 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 | * 所有先前使用者的登入資訊存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用時，則仍然可以登入 * 如果網域控制站無法使用，且未快取使用者的登入資訊時，則會提示使用者下列訊息：「目前無可用的登入伺服器來服務登入請求」 * 在此原則設定中，零值會停用登入快取。若值超過50，則只會快取50次登入嘗試 | 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：網域控制站無法使用時，要快取的先前登入次數 | 2次 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0113 | 安全性選項\互動式登入 | 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 | * 所有先前使用者的登入資訊存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用時，則仍然可以登入 * 如果網域控制站無法使用，且未快取使用者的登入資訊時，則會提示使用者下列訊息：「目前無可用的登入伺服器來服務登入請求」 * 在此原則設定中，零值會停用登入快取。若值超過50，則只會快取50次登入嘗試 | 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：網域控制站無法使用時，要快取的先前登入次數 | 2次以下 |
| 42 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0114 | 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 | 此項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先提醒使用者 | 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 | 14天 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0114 | 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 | 此項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先提醒使用者 | 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 | 14天以上 |
| 43 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0117 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(自動) | * 此安全性設定決定SMB用戶端元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此原則設定決定允許和SMB伺服器進一步通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此設定，Microsoft網路用戶端將不會和Microsof網路伺服器通訊，除非該伺服器同意執行SMB封包簽章。若停用此原則，會在用戶端和伺服器之間交涉SMB封包簽章 * 重要：使此原則在執行Windows 2000的電腦上生效，必須也啟用用戶端封包簽章。若要啟用用戶端SMB封包簽章，請設定「Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)」 * 已設定此原則的電腦將無法和未啟用伺服器端封包簽章的電腦通訊。根據預設值，只會在執行Windows 2000或更新版本的網域控制站上啟用伺服器端封包簽章 * 在執行Windows 2000作業系統，且已啟用「Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)」的電腦上，可啟用伺服器端封包簽章 * 將下列登錄值設為1，可在執行Windows NT 4.0 Service Pack 3及更新版本的電腦上啟用伺服器端封包簽章：HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature * 伺服器端封包簽章無法在執行Windows 95或Windows 98的電腦上啟用 * 注意：有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。若要發揮SMB封包簽章的功能，涉及通訊的用戶端SMB元件和伺服器端SMB元件必須啟用或要求SMB封包簽章。在Windows 2000及更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列四個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若伺服器端SMB簽章是必要的，除非啟用用戶端SMB簽章，否則用戶端將無法和該伺服器建立工作階段。根據預設值，用戶端SMB簽章在工作站、伺服器及網域控制站中為啟用。同樣的，若用戶端SMB簽章是必要的，該用戶端將無法和未啟用封包簽章的伺服器建立工作階段。根據預設值，伺服器端SMB簽章只會在網域控制站中啟用 * 若啟用伺服器端SMB簽章，則將與啟用用戶端SMB簽章的用戶端交涉SMB封包簽章 * 使用SMB封包簽章最多會造成檔案服務交易的效能降低15% | 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：數位簽章用戶端的通訊(自動) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0117 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(自動) | * 此安全性設定決定SMB用戶端元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此原則設定決定允許和SMB伺服器進一步通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此原則，Microsoft網路用戶端將不會和Microsof網路伺服器通訊，除非該伺服器同意執行SMB封包簽章 * 若停用此原則，會在用戶端和伺服器之間交涉SMB封包簽章 * 重要：使此原則在執行Windows 2000的電腦上生效，必須也啟用用戶端封包簽章。若要啟用用戶端SMB封包簽章，請設定「Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)」 * 注意：所有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。在Windows 2000及更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低 | 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：數位簽章用戶端的通訊(自動) | 啟用 |
| 44 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0118 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意) | * 此項原則設定決定SMB用戶端是否嘗試交涉SMB封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章 * 此項原則設定決定SMB用戶端元件連線至SMB伺服器時，是否嘗試交涉SMB封包簽章 * 若啟用此設定，Microsoft網路用戶端將於建立工作階段時要求伺服器執行SMB封包簽章。若已在伺服器上啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。若要發揮SMB封包簽章的功能，涉及通訊的用戶端SMB元件與伺服器端SMB元件必須啟用或要求SMB封包簽章。在Windows2000和更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若伺服器端SMB簽章是必要的，除非啟用用戶端SMB簽章，否則用戶端將無法與該伺服器建立工作階段。根據預設值，用戶端SMB簽章在工作站、伺服器及網域控制站中為啟用 * 同樣的，若用戶端SMB簽章是必要的，該用戶端將無法和未啟用封包簽章的伺服器建立工作階段。根據預設值，伺服器端SMB簽章只會在網域控制站中啟用。若啟用伺服器端SMB簽章，則將與啟用用戶端SMB簽章的用戶端交涉SMB封包簽章 * 使用SMB封包簽章最多會造成檔案服務交易的效能降低15% | 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：數位簽章用戶端的通訊(如果伺服器同意) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0118 | 安全性選項\Microsoft網路用戶端 | Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意) | * 此項原則設定決定SMB用戶端是否嘗試交涉SMB封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章 * 此項原則設定決定SMB用戶端元件連線至SMB伺服器時，是否嘗試交涉SMB封包簽章 * 若啟用此設定，Microsoft網路用戶端將於建立工作階段時要求伺服器執行SMB封包簽章。若已在伺服器上啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件和伺服器端SMB元件。在Windows2000和更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若用戶端與伺服器端SMB簽章兩者已啟用，且用戶端將建立與伺服器之間的SMB 1.0連線，將會嘗試SMB簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低。此設定只適用於SMB 1.0連線 | 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：數位簽章用戶端的通訊(如果伺服器同意) | 啟用 |
| 45 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0120 | 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 | * 此項原則設定決定伺服器訊息區(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 * 系統管理員可使用此原則，控制電腦於何時暫停非使用中的SMB工作階段。若用戶端活動繼續，則會自動重新建立工作階段 * 設定為零值表示在合理的時間範圍內儘速中斷工作階段的連線。最大值是99,999，即208天，實際上，此值會停用此原則 | 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 | 15分鐘 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0120 | 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 | * 此項原則設定決定伺服器訊息區(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 * 系統管理員可使用此原則，控制電腦於何時暫停非使用中的SMB工作階段。若用戶端活動繼續，則會自動重新建立工作階段 * 設定為零值表示在合理的時間範圍內儘速中斷工作階段的連線。最大值是99,999，實際上，此值會停用此原則 | 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 | 15分鐘以下，但須大於0分鐘 |
| 46 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0121 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(自動) | * 此項原則設定決定SMB伺服器元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定允許和SMB用戶端進行進一步的通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此設定，Microsoft網路伺服器將不會與Microsoft網路用戶端通訊，除非該用戶端同意執行SMB封包簽章 * 若停用此設定，會在用戶端與伺服器之間交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。若要發揮SMB封包簽章的功能，涉及通訊的用戶端SMB元件與伺服器端SMB元件必須啟用或要求SMB封包簽章。在Windows 2000與更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若伺服器端SMB簽章是必要的，除非啟用用戶端SMB簽章，否則用戶端將無法與該伺服器建立工作階段。根據預設值，用戶端SMB簽章在工作站、伺服器及網域控制站中為啟用 * 同樣的，若用戶端SMB簽章是必要的，該用戶端將無法與未啟用封包簽章的伺服器建立工作階段。根據預設值，伺服器端SMB簽章只會在網域控制站中啟用 * 若啟用伺服器端SMB簽章，則將與啟用用戶端SMB簽章的用戶端交涉SMB封包簽章 * 使用SMB封包簽章最多會造成檔案服務交易的效能降低15% | 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：數位簽章伺服器的通訊(自動) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0121 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(自動) | * 此項原則設定決定SMB伺服器元件是否需要封包簽章 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定允許和SMB用戶端進行進一步的通訊之前，SMB封包簽章是否必須經過交涉 * 若啟用此設定，Microsoft網路伺服器將不會與Microsoft網路用戶端通訊，除非該用戶端同意執行SMB封包簽章 * 若停用此設定，會在用戶端與伺服器之間交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。在Windows 2000與更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 同樣的，若用戶端SMB簽章是必要的，該用戶端將無法與未啟用封包簽章的伺服器建立工作階段。根據預設值，伺服器端SMB簽章只會在網域控制站中啟用 * 若啟用伺服器端SMB簽章，則將與啟用用戶端SMB簽章的用戶端交涉SMB封包簽章 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低 | 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：數位簽章伺服器的通訊(自動) | 啟用 |
| 47 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0122 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意) | * 此項原則設定決定SMB伺服器是否將和要求SMB封包簽章的用戶端交涉 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定SMB伺服器是否將在SMB用戶端要求SMB封包簽章時進行交涉 * 若啟用此設定，Microsoft網路伺服器將在用戶端要求SMB封包簽章時進行交涉。也就是說，若已在用戶端啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 | 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：數位簽章伺服器的通訊(如果用戶端同意) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0122 | 安全性選項\Microsoft網路伺服器 | Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意) | * 此項原則設定決定SMB伺服器是否將和要求SMB封包簽章的用戶端交涉 * 伺服器訊息區(SMB)通訊協定是Microsoft檔案及列印共用和許多其他網路作業(例如遠端Windows系統管理)的基礎。為避免攔截式攻擊修改傳送中的SMB封包，SMB通訊協定支援SMB封包的數位簽章。此項原則設定決定SMB伺服器是否將在SMB用戶端要求SMB封包簽章時進行交涉 * 若啟用此設定，Microsoft網路伺服器將在用戶端要求SMB封包簽章時進行交涉。也就是說，若已在用戶端啟用封包簽章，將會交涉封包簽章 * 若停用此原則，SMB用戶端將不會交涉SMB封包簽章 * 注意：所有Windows作業系統都支援用戶端SMB元件與伺服器端SMB元件。在Windows 2000與更新版本的作業系統上，啟用或要求用戶端與伺服器端SMB元件的封包簽章是由下列4個原則設定所控制： * Microsoft網路用戶端：數位簽章用戶端的通訊(自動)-控制用戶端SMB元件是否需要封包簽章 * Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)-控制用戶端SMB元件是否啟用封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(自動)-控制伺服器端SMB元件是否需要封包簽章 * Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)-控制伺服器端SMB元件是否啟用封包簽章 * 若用戶端與伺服器端SMB簽署兩者已啟用，且用戶端建立與伺服器之間的SMB 1.0連線，將會嘗試SMB簽署 * 視方言版本、OS版本、檔案大小、處理器卸載功能與應用程式IO行為而定，SMB封包簽署會使SMB效能大幅降低。此設定只適用於SMB 1.0連線 | 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：數位簽章伺服器的通訊(如果用戶端同意) | 啟用 |
| 48 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0125 | 安全性選項\MSS | MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | * 此項原則設定決定電腦是否採取自動登入方式 * 如果設定為啟用：當電腦啟動時，將使用以純文字形式儲存於Registry內之網域、帳號及密碼資訊自動登入該電腦，因此能實體存取電腦的任何人也都能存取該電腦中的一切資訊，包括任何網路或電腦所能連線到的網路在內 * 如果設定為停用：電腦將不採取自動登入方式 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0125 | MSS(Legacy) | MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | * 此項原則設定決定電腦是否採取自動登入方式 * 如果設定為啟用，當電腦啟動時，將使用以純文字形式儲存於Registry內之網域、帳號及密碼資訊自動登入該電腦，因此能實體存取電腦的任何人也都能存取該電腦中的一切資訊，包括任何網路或電腦所能連線到的網路在內 * 如果設定為停用，電腦將不採取自動登入方式 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | 停用 |
| 49 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0126 | 安全性選項\MSS | MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | * IP source routing可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection：代表作業系統接受與轉送來源路由封包 * 設為Medium，代表作業系統接受但不轉送來源路由封包 * 設為Highestprotection，代表作業系統完全拒絕來源路由封包 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | Highest protection，source routing is completely disabled |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0126 | MSS(Legacy) | MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | * IP source routing可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection, source routed packets are allowed：代表作業系統接受與轉送來源路由封包 * 設為Medium, source routed packets ignored when IP forwarding is enabled，代表作業系統接受但不轉送來源路由封包 * 設為Highestprotection, source routing is completely disabled，代表作業系統完全拒絕來源路由封包 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | 啟用，Highest protection, source routing is completely disabled |
| 50 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0127 | 安全性選項\MSS | MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | * IP source routing是一種允許傳送者決定資料包通過網路時應該採用IP路由的機制，可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection：代表作業系統接受與轉送來源路由封包 * 設為Medium，代表作業系統接受但不轉送來源路由封包 * 設為Highestprotection，代表作業系統完全拒絕來源路由封包 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | Highest protection, source routing is completely disabled |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0127 | MSS(Legacy) | MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | * IP source routing是一種允許傳送者決定資料包通過網路時應該採用IP路由的機制，可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 * 此項原則設定決定IP source routing防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： * 設為No additional protection, source routed packets are allowed：代表作業系統接受與轉送來源路由封包 * 設為Medium, source routed packets ignored when IP forwarding is enabled，代表作業系統接受但不轉送來源路由封包 * 設為Highestprotection, source routing is completely disabled，代表作業系統完全拒絕來源路由封包 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | 啟用，Highest protection, source routing is completely disabled |
| 51 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0128 | 安全性選項\MSS | MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | * 此項原則設定決定是否允許ICMP重新導向覆寫OSPF產生的路由，意謂著作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，是否要改變其路由表 * 如果設定為啟用：作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，將會改變其路由表 * 如果設定為停用：作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，不會改變其路由表 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0128 | MSS(Legacy) | MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | * 此項原則設定決定是否允許ICMP重新導向覆寫OSPF產生的路由，意謂著作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，是否要改變其路由表 * 如果設定為啟用，作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，將會改變其路由表 * 如果設定為停用，作業系統在回應由網路裝置(例如路由器)傳送給它的ICMP重新導向訊息時，不會改變其路由表 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 停用 |
| 52 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0129 | 安全性選項\MSS | MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | * 此項原則設定決定是否從網路瀏覽列表中移除本台電腦名稱 * 如果設定為啟用：將從網路瀏覽列表中移除本台電腦名稱 * 如果設定為停用：網路瀏覽列表依然保留本台電腦名稱。知道本台電腦名稱之攻擊者，將可能透過網路蒐集本台電腦資訊 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0129 | MSS(Legacy) | MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | * 此項原則設定決定是否從網路瀏覽列表中移除本台電腦名稱 * 如果設定為啟用，將從網路瀏覽列表中移除本台電腦名稱 * 如果設定為停用，網路瀏覽列表依然保留本台電腦名稱。知道本台電腦名稱之攻擊者，將可能透過網路蒐集本台電腦資訊 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | 啟用 |
| 53 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0130 | 安全性選項\MSS | MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | * 此項原則設定決定持續作用的封包多少毫秒會傳送一次，讓TCP藉由傳送持續作用封包，來嘗試驗證閒置連線狀態是否仍然不變 * 如果遠端系統仍然可以連接與運作，就會確認持續作用傳輸在預設的情況下，並不會傳送持續作用封包 * 此項功能可由應用程式在連線時啟用 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | 300000或5分鐘 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0130 | MSS(Legacy) | MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | * 此項原則設定決定持續作用的封包多少毫秒會傳送一次，讓TCP藉由傳送持續作用封包，來嘗試驗證閒置連線狀態是否仍然不變 * 如果遠端系統仍然可以連接與運作，就會確認持續作用傳輸在預設的情況下，並不會傳送持續作用封包 * 此項功能可由應用程式在連線時啟用 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | 啟用，300000或5分鐘 |
| 54 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0131 | 安全性選項\MSS | MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | * 此項原則設定決定是否啟用IPSec篩選器的預設豁免項目 選項如下： * 設定為0：代表「多點傳送廣播，RSVP、Kerberos及ISAKMP流量不受限於IPSec篩選功能」 * 設定為1：代表「Kerberos及RSVP流量並不受IPSec篩選，但多點傳播、廣播及ISAKMP流量都是豁免」 * 設定為2：代表「多點傳播和廣播流量並不受IPSec篩選，但RSVP、Kerberos及ISAKMP流量被豁免」 * 設定為3：代表「只有ISAKMP流量是免除IPSec篩選功能」 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | Multicast，broadcast，and ISAKMP are exempt(Best for Windows XP) |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0131 | MSS(Legacy) | MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | * 此項原則設定決定是否啟用IPSec篩選器的預設豁免項目，選項如下： * Allow all exemptions (least secure)：代表「多點傳送廣播，RSVP、Kerberos及ISAKMP流量不受限於IPSec篩選功能」 * Multicast, broadcast, & ISAKMP exempt (best for Windows XP)：代表「Kerberos及RSVP流量並不受IPSec篩選，但多點傳播、廣播及ISAKMP流量都是豁免」 * RSVP, Kerberos, and ISAKMP are exempt：代表「多點傳播和廣播流量並不受IPSec篩選，但RSVP、Kerberos及ISAKMP流量被豁免」 * Only ISAKMP is exempt (recommended for Windows Server 2003)：代表「只有ISAKMP流量是免除IPSec篩選功能」 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | 啟用，Multicast，broadcast，and ISAKMP are exempt(best for Windows XP) |
| 55 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0132 | 安全性選項\MSS | MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | * NetBIOS(網路基本輸入/輸出系統)overTCP/IP是一種網路通訊協定，提供簡易的解析方法，可以將登錄在Windows系統上的NetBIOS名稱解析為這些系統所設定的IP位址 * 此項原則設定決定當電腦收到名稱釋放要求時是否釋放它的NetBIOS名稱 * 如果設定為啟用：當電腦收到名稱釋放要求時，不會釋放它的NetBIOS名稱 * 如果設定為停用：當電腦收到名稱釋放要求時，將會釋放它的NetBIOS名稱。惡意的使用者可以利用此通訊協定不需驗證的特質，將名稱衝突的資料包傳送到目標電腦，造成名稱釋放的情形而停止回應查詢，造成目標電腦發生連線斷斷續續的問題，或甚至造成無法使用「網路上的芳鄰」、網域登入、netsend命令，或是無法進行後續的NetBIOS名稱解析 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0132 | MSS(Legacy) | MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | * NetBIOS(網路基本輸入/輸出系統)overTCP/IP是一種網路通訊協定，提供簡易的解析方法，可以將登錄在Windows系統上的NetBIOS名稱解析為這些系統所設定的IP位址 * 此項原則設定決定當電腦收到名稱釋放要求時是否釋放它的NetBIOS名稱 * 如果設定為啟用，當電腦收到名稱釋放要求時，不會釋放它的NetBIOS名稱 * 如果設定為停用，當電腦收到名稱釋放要求時，將會釋放它的NetBIOS名稱。惡意的使用者可以利用此通訊協定不需驗證的特質，將名稱衝突的資料包傳送到目標電腦，造成名稱釋放的情形而停止回應查詢，造成目標電腦發生連線斷斷續續的問題，或甚至造成無法使用「網路上的芳鄰」、網域登入、netsend命令，或是無法進行後續的NetBIOS名稱解析 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | 啟用 |
| 56 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0133 | 安全性選項\MSS | MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | * 此項原則設定決定是否允許Internet Router Discovery Protocol(IRDP)自動偵測與設定預設Gateway位址 * 設定選項如下： * 停用 * 啟用 * 僅在DHCP傳送路由器探查選項時啟用 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0133 | MSS(Legacy) | MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 此項原則設定決定是否允許Internet Router Discovery Protocol(IRDP)自動偵測與設定預設Gateway位址 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 停用 |
| 57 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0134 | 安全性選項\MSS | MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | * 此項原則設定決定應用程式搜尋DLL檔的順序 * 如果設定為啟用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 目前目錄 * 在PATH環境變數中列出來的目錄 * 如果設定為停用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 目前目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 在PATH環境變數中列出來的目錄 | 電腦設定\ Windows設定\安全性設定\本機原則\安全性選項\MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0134 | MSS(Legacy) | MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | * 此項原則設定決定應用程式搜尋DLL檔的順序 * 如果設定為啟用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 目前目錄 * 在PATH環境變數中列出來的目錄 * 如果設定為停用，搜尋DLL的順序如下： * 應用程式被載入的目錄 * 目前目錄 * 系統目錄 * 16位元系統目錄(如果有的話) * Windows目錄 * 在PATH環境變數中列出來的目錄 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | 啟用 |
| 58 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0135 | 安全性選項\MSS | MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | * 若啟用螢幕保護裝置的鎖定功能，在螢幕保護裝置啟動到主控台實際自動鎖定之間，Windows設置有一段寬限期。此項原則設定決定寬限期時間(以秒計算) * 可以設定為介於0到255之間的任何數值 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 5 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0135 | MSS(Legacy) | MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | * 若啟用螢幕保護裝置的鎖定功能，在螢幕保護裝置啟動到主控台實際自動鎖定之間，Windows設置有一段寬限期。此項原則設定決定寬限期時間(以秒計算) * 可以設定為介於0到255之間的任何數值 | 電腦設定\系統管理範本\MSS(Legacy)\ MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 啟用，5以下，但須大於0 |
| 59 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0136 | 安全性選項\MSS | MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0136 | MSS(Legacy) | MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 啟用，3以下，但須大於0 |
| 60 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0137 | 安全性選項\MSS | MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0137 | MSS(Legacy) | MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | * 此項原則設定決定在放棄連線之前，透過TCP重傳未獲回應之資料的次數 * 建議值設為3次，預設值設為5次 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 啟用，3以下，但須大於0 |
| 61 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0138 | 安全性選項\MSS | MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | * 當安全性事件記錄檔大小到達最大可用的百分比時，產生警告 * 預設值沒有指定，當定義此原則時，可以選擇50%、60%、70%、80%或90%等臨界值 * 如果安全性事件記錄檔設定為覆寫，則不會產生警告 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | 90 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0138 | MSS(Legacy) | MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | * 當安全性事件記錄檔大小到達最大可用的百分比時，產生警告 * 預設值沒有指定，當定義此原則時，可以選擇50%、60%、70%、80%或90%等臨界值 * 如果安全性事件記錄檔設定為覆寫，則不會產生警告 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | 啟用，90 |
| 62 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0139 | 安全性選項\MSS | MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 此項原則決定當使用撥接網路或VPN連接撥接網路時，可以選擇「儲存密碼」以便快取撥接網路密碼，不需要再連續嘗試撥接時輸入 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0139 | MSS(Legacy) | MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 此項原則決定當使用撥接網路或VPN連接撥接網路時，可以選擇「儲存密碼」以便快取撥接網路密碼，不需要再連續嘗試撥接時輸入 | 電腦設定\系統管理範本\MSS(Legacy)\MSS：(DisableSavePassword) Prevent the dial-up password from being saved (recommended) | 啟用 |
| 63 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0142 | 安全性選項\網路存取 | 網路存取：不允許SAM帳戶的匿名列舉 | * 此項原則設定決定授與電腦匿名連線哪些其他權限 * Windows允許匿名使用者執行特定活動，例如列舉網域帳戶和網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權，而該網域不會保持交互信任時，此功能相當方便。如果想禁止SAM帳戶和共用的匿名列舉，請啟用此原則 | 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 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0142 | 安全性選項\網路存取 | 網路存取：不允許SAM帳戶的匿名列舉 | * 此項原則設定決定授與電腦匿名連線哪些其他權限 * Windows允許匿名使用者執行特定活動，例如列舉網域帳戶和網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權，而該網域不會保持交互信任時，此功能相當方便。如果想禁止SAM帳戶和共用的匿名列舉，請啟用此原則 * 此安全性選項允許在匿名連線中設定其他限制，如下： * 啟用：不允許列舉SAM帳戶。此選項會將資源之安全性權限中的Everyone取代為Authenticated Users * 停用：沒有其他限制。視預設權限而定 | 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 | 啟用 |
| 64 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0148 | 安全性選項\網路存取 | 網路存取：限制匿名存取具名管道和共用 | * 啟用此項原則設定時，會將共用和管道的匿名存取限制為以下設定： * 網路存取：可以匿名存取的具名管道 * 網路存取：可以匿名存取的共用 | 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：限制匿名存取具名管道和共用 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0148 | 安全性選項\網路存取 | 網路存取：限制匿名存取具名管道和共用 | * 此項原則設定決定是否限制匿名存取具名管道和共用 * 啟用時，此項原則設定會將共用和管道的匿名存取限制為以下設定： * 網路存取：可以匿名存取的具名管道 * 網路存取：可以匿名存取的共用 | 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：限制匿名存取具名管道和共用 | 啟用 |
| 65 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0151 | 安全性選項\網路安全性 | 網路安全性：允許Local System對NTLM使用電腦身分識別 | * 此項原則設定允許使用交涉的Local System服務在還原使用NTLM驗證時，使用電腦身分識別 * 如果啟用此項原則設定，以Local System執行且使用交涉的服務會使用電腦身分識別。這可能會造成Windows作業系統之間的某些驗證要求失敗並記錄錯誤 * 如果未設定此項原則設定，則以Local System執行且使用交涉的服務在還原為NTLM驗證時將會匿名驗證。這是舊版Windows中的預設作法 * 作業系統必須至少是Windows 7或Windows Server 2008 R2才支援此原則 | 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：允許Local System對NTLM使用電腦身分識別 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0151 | 安全性選項\網路安全性 | 網路安全性：允許Local System對NTLM使用電腦身分識別 | * 此項原則設定允許使用交涉的Local System服務在還原使用NTLM驗證時，使用電腦身分識別 * 如果啟用此項原則設定，以Local System執行且使用交涉的服務會使用電腦身分識別。這可能會造成Windows作業系統之間的某些驗證要求失敗並記錄錯誤 * 如果停用此項原則設定，則以Local System執行且使用交涉的服務在還原為NTLM驗證時將會匿名驗證。 | 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：允許Local System對NTLM使用電腦身分識別 | 啟用 |
| 66 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0153 | 安全性選項\網路安全性 | 網路安全性：允許對此電腦的PKU2U驗證要求使用線上身分識別 | 在已加入網域的電腦上預設會關閉此原則。這樣便不會允許使用線上身分識別來向已加入網域的電腦驗證 | 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：允許對此電腦的PKU2U驗證要求使用線上身分識別 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0153 | 安全性選項\網路安全性 | 網路安全性：允許對此電腦的PKU2U驗證要求使用線上身分識別 | * 在已加入網域的電腦上預設會關閉此原則。這樣便不會允許使用線上身分識別來向已加入網域的電腦驗證 * 在Windows 10 1607版前，此原則在已加入網域的電腦上預設為停用，在1607版後，此原則預設為啟用 | 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：允許對此電腦的PKU2U驗證要求使用線上身分識別 | 停用 |
| 67 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0154 | 安全性選項\網路安全性 | 網路安全性：設定Kerberos允許的加密類型 | * 此項原則將設定允許Kerberos使用的加密類型 * 如果未選取，則不允許加密類型。此項設定可能會影響與用戶端電腦或服務及應用程式的相容性 * 此項原則設定允許多個選取項目，作業系統平台必須至少是Windows 7或Windows Server 2008 R2才支援此原則設定 | 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 | * RC4\_HMAC\_MD5 * AES128\_HMAC\_SHA1 * AES256\_HMAC\_SHA1   未來的加密類型 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0154 | 安全性選項\網路安全性 | 網路安全性：設定Kerberos允許的加密類型 | * 此項原則將設定允許Kerberos使用的加密類型 * 如果未選取，則不允許加密類型。此項設定可能會影響與用戶端電腦或服務及應用程式的相容性 * 此項原則設定允許多個選取項目 | 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 | * AES128\_HMAC\_SHA1 * AES256\_HMAC\_SHA1   未來的加密類型 |
| 68 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0159 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 此項原則設定允許用戶端要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，選項如下： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0159 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 此項原則設定允許用戶端要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，可勾選的安全性設定值選項如下(可複選)： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 |
| 69 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0160 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 此項原則設定允許伺服器要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，選項如下： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0160 | 安全性選項\網路安全性 | 網路安全性：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 此項原則設定允許伺服器要求128位元加密和/或NTLMv2工作階段安全性的交涉。這些值依存於LAN Manager驗證等級安全性設定值，可勾選的安全性設定值選項如下(可複選)： * 要求NTLMv2工作階段安全性：若未交涉NTLMv2通訊協定，連線將會失敗 * 要求128位元加密：若未交涉增強式加密(128位元)，連線將會失敗 | 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：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | * 要求NTLMv2工作階段安全性 * 要求128位元加密 |
| 70 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0165 | 安全性選項\系統加密編譯 | 系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | * 對於Schannel Security Service Provider(SSP)，此項原則設定會停用強度較低的安全通訊端層(SSL)通訊協定，而且只支援傳輸層安全性(TLS)通訊協定作為用戶端以及伺服器(如果適用)連線機制 * 如果啟用此設定，傳輸層安全性/安全通訊端層(TLS/SSL)安全性提供者只會使用FIPS140核准的密碼編譯演算法：3DES與AES用於加密、RSA或ECC公開金鑰密碼編譯用於TLS金鑰交換與驗證，而且只有安全雜湊演算法(SHA1、SHA256、SHA384以及SHA512)用於TLS雜湊需求 * 對於加密檔案系統服務(EFS)，僅支援使用三重資料加密標準(DES)與進階加密標準(AES)加密演算法來加密NTFS檔案系統支援的檔案資料 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0165 | 安全性選項\系統加密編譯 | 系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | * 對於Schannel Security Service Provider(SSP)，此項原則設定會停用強度較低的安全通訊端層(SSL)通訊協定，而且只支援傳輸層安全性(TLS)通訊協定作為用戶端以及伺服器(如果適用)連線機制 * 如果啟用此設定，傳輸層安全性/安全通訊端層(TLS/SSL)安全性提供者只會使用FIPS140核准的密碼編譯演算法：3DES與AES用於加密、RSA或ECC公開金鑰密碼編譯用於TLS金鑰交換與驗證，而且只有安全雜湊演算法(SHA1、SHA256、SHA384以及SHA512)用於TLS雜湊需求 * 對於加密檔案系統服務(EFS)，僅支援使用三重資料加密標準(DES)與進階加密標準(AES)加密演算法來加密NTFS檔案系統支援的檔案資料 * 對於遠端桌面服務，它只支援使用三重DES加密演算法來加密遠端桌面服務網路通訊 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統密碼編譯：使用FIPS相容演算法於加密、雜湊以及簽章 | 啟用 |
| 71 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0166 | 安全性選項\系統物件 | 系統物件：要求不區分大小寫用於非Windows子系統 | * 此項原則設定決定是否要強制所有子系統區分大小寫。Win32子系統不會區分大小寫。但是如POSIX等其他子系統的核心支援區分大小寫 * 如果啟用此設定，便會強制所有目錄物件、符號連結及IO物件(包括檔案物件在內)區分大小寫 * 停用此設定將不允許Win32子系統區分大小寫 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統物件：要求不區分大小寫用於非Windows子系統 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0166 | 安全性選項\系統物件 | 系統物件：要求不區分大小寫用於非Windows子系統 | * 此項原則設定決定是否要強制所有子系統區分大小寫。Win32子系統不會區分大小寫。但是如POSIX等其他子系統的核心支援區分大小寫 * 如果啟用此設定，便會強制所有目錄物件、符號連結及IO物件(包括檔案物件在內)不區分大小寫 * 如果停用此設定，將允許非Windows子系統區分大小寫 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\系統物件：要求不區分大小寫用於非Windows子系統 | 啟用 |
| 72 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0170 | 安全性選項\使用者帳戶控制 | 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 | * 此原則設定會控制系統管理員之提升權限提示的行為，選項如下： * 提升權限而不提示：允許具有特殊權限的帳戶執行需要提升權限的操作，而不需同意或是認證。注意：請只在最嚴謹的環境中使用此選項 * 在安全桌面提示輸入認證：當操作需要提升權限時，會在安全桌面提示使用者輸入具有特殊權限的使用者名稱與密碼。如果使用者輸入有效的認證，操作會以使用者的最高可用權限繼續 * 在安全桌面提示要求同意：當操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 認證提示：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 同意提示：當操作需要提升權限時，會提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 非Windows二進位檔案的同意提示：(預設值)當非Microsoft應用程式的操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 | 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 | 在安全桌面提示要求同意 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0170 | 安全性選項\使用者帳戶控制 | 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 | * 此原則設定會控制系統管理員之提升權限提示的行為，選項如下： * 提升權限而不提示：允許具有特殊權限的帳戶執行需要提升權限的操作，而不需同意或是認證。注意：請只在最嚴謹的環境中使用此選項 * 在安全桌面提示輸入認證：當操作需要提升權限時，會在安全桌面提示使用者輸入具有特殊權限的使用者名稱與密碼。如果使用者輸入有效的認證，操作會以使用者的最高可用權限繼續 * 在安全桌面提示要求同意：當操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 提示輸入認證：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 提示要求同意：當操作需要提升權限時，會提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 * 提示要求同意非Windows二進位檔案：(預設值)當非Microsoft應用程式的操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 | 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 | 在安全桌面提示要求同意 |
| 73 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0171 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：標準使用者之提高權限提示的行為 | * 此項原則設定會控制標準使用者之提升權限提示的行為，選項如下： * 認證提示：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。若使用者輸入有效的認證，該操作會以適用的權限繼續執行 * 自動拒絕提升權限要求：當操作需要提升權限時，會顯示可設定的存取拒絕錯誤訊息。以標準使用者身分執行桌上型電腦的機關可能會選擇此設定，以降低需要尋求支援部門協助的機會 * 在安全桌面提示輸入認證：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。如果使用者輸入有效的認證，操作會以適用的權限繼續 | 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：標準使用者之提高權限提示的行為 | 在安全桌面顯示輸入認證 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0171 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：標準使用者之提高權限提示的行為 | * 此項原則設定會控制標準使用者之提升權限提示的行為，選項如下： * 提示輸入認證(預設值)：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。若使用者輸入有效的認證，該操作會以適用的權限繼續執行 * 自動拒絕提升權限要求：當操作需要提升權限時，會顯示拒絕存取錯誤訊息。以標準使用者身分執行桌上型電腦的機關可能會選擇此設定，以降低需要尋求支援部門協助的機會 * 在安全桌面提示輸入認證：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。如果使用者輸入有效的認證，操作會以適用的權限繼續執行 | 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：標準使用者之提高權限提示的行為 | 在安全桌面提示輸入認證 |
| 74 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0172 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：偵測應用程式安裝，並提示提高權限 | * 此項原則設定會控制電腦的應用程式安裝偵測行為，選項如下: * 已啟用(預設值)：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。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 已停用：未偵測到應用程式安裝封裝，也未提示提升權限。執行標準使用者桌面並利用委派安裝技術(例如，群組原則軟體安裝或Systems Management Server (SMS))的機關，應該停用此原則設定。在此情況下，不需要進行安裝程式偵測 | 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，並提示提高權限 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0172 | 安全性選項\使用者帳戶控制 | 使用者帳戶控制：偵測應用程式安裝，並提示提升權限 | * 此項原則設定會控制電腦的應用程式安裝偵測行為，選項如下： * 啟用(預設值)：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。如果使用者輸入有效的認證，操作會以適用的權限繼續 * 停用：未偵測到應用程式安裝封裝，也未提示提升權限。執行標準使用者桌面並利用委派安裝技術(例如，群組原則軟體安裝或Systems Management Server (SMS))的機關，應該停用此原則設定。在此情況下，不需要進行安裝程式偵測 | 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 | 啟用 |
| 75 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0206 | 使用者權限指派 | 以批次工作登入 | 此項原則設定允許使用者以批次工作登入，且僅提供與舊版Windows相容之用，例如：當使用者以工作排程器提交工作時，工作排程器會以批次使用者登入該使用者，而不是互動式使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\以批次工作登入 | No One |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0206 | 使用者權限指派 | 以批次工作登入 | 此項原則設定允許使用者以批次佇列設備登入，且僅提供與舊版Windows相容之用，例如：當使用者以工作排程器提交工作時，工作排程器會以批次使用者登入該使用者，而不是互動式使用者 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\以批次工作登入 | No One |
| 76 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0218 | 使用者權限指派 | 同步處理目錄服務資料 | 此項原則設定決定授權哪些使用者及群組同步處理所有目錄服務資料，此項原則設定亦稱為Active Directory同步處理 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\同步處理目錄服務資料 | 無 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0218 | 使用者權限指派 | 同步處理目錄服務資料 | 此項原則設定決定授權哪些使用者及群組同步處理所有目錄服務資料，此項原則設定亦稱為Active Directory同步處理 | 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\同步處理目錄服務資料 | No one |
| 77 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0223 | Windows元件 | 設定AutoRun的預設行為 | * 此項原則設定可設定Auto Run命令的預設行為 * 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常式 * 在Windows Vista之前，在插入含有AutoRun命令的媒體時，系統會自動執行程式，而不需使用者介入 * 這會產生主要的安全性考量，因為程式碼可能會在使用者不知情的情況下執行。從Windows Vista開始的預設行為是，提示使用者是否要執行AutoRun命令 * Auto Run命令會呈現為「自動播放」對話方塊中的處理常式 * 如果啟用此項原則設定，系統管理員可以將Windows Vista或更新版本的AutoRun預設行為變更為下列行為： * 完全停用AutoRun命令，或者 * 轉換回Windows Vista之前的行為，自動執行AutoRun命令 * 如果停用或未設定此項原則設定，Windows Vista或更新版本將會提示使用者是否要執行AutoRun命令 | 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 | 啟用，不執行任何AutoRun命令 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0223 | Windows元件 | 設定AutoRun的預設行為 | * 此項原則設定可設定Auto Run命令的預設行為 * 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常式 * 在Windows Vista之前，在插入含有AutoRun命令的媒體時，系統會自動執行程式，而不需使用者介入 * 這會產生主要的安全性考量，因為程式碼可能會在使用者不知情的情況下執行。從Windows Vista開始的預設行為是，提示使用者是否要執行AutoRun命令 * Auto Run命令會呈現為「自動播放」對話方塊中的處理常式 * 如果啟用此項原則設定，系統管理員可以將Windows Vista或更新版本的AutoRun預設行為變更為下列行為： * 完全停用AutoRun命令，或者 * 轉換回Windows Vista之前的行為，自動執行AutoRun命令 * 如果停用或未設定此項原則設定，Windows Vista或更新版本將會提示使用者是否要執行AutoRun命令 | 電腦設定\系統管理範本\Windows元件\自動播放原則\設定Autorun的預設行為 | 啟用，不執行任何AutoRun命令 |
| 78 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0229 | Windows元件 | 停用Windows錯誤報告 | * 如果啟用此項原則設定，Windows錯誤報告不會傳送任何問題資訊到Microsoft * 「行動作業中心」控制台中的解決方案資訊將無法使用 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\停用Windows錯誤報告 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0229 | Windows元件 | 停用Windows錯誤報告 | * 此項原則設定會關閉Windows錯誤報告，因此當軟體發生未預期的停止或失敗時，不會收集或傳送報告給Microsoft或機關內的內部伺服器 * 如果啟用此項原則設定，Windows錯誤報告不會傳送任何問題資訊到Microsoft。此外，「控制台」的「安全性與維護」不會提供解決方案的資訊 * 如果停用或未設定此項原則設定，則「電腦設定/系統管理範本/系統/網際網路通訊管理/網際網路通訊/關閉Windows錯誤報告」原則設定的優先順序最高 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\停用Windows錯誤報告 | 啟用 |
| 79 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0230 | Windows元件 | 不傳送其他資料 | 如果此項原則設定已啟用，則不會通知使用者而自動拒絕回應「Windows錯誤報告」事件時Microsoft所要求的任何其他資料 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\不傳送其他資料 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0230 | Windows元件 | 不傳送其他資料 | * 此項原則設定決定支援錯誤報告的其他資料是否可以自動傳送到Microsoft * 如果啟用此項原則設定，則不會通知使用者而自動拒絕回應「Windows錯誤報告」事件時Microsoft所要求的任何其他資料 | 電腦設定\系統管理範本\Windows元件\Windows錯誤報告\不傳送其他資料 | 啟用 |
| 80 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0243 | Windows元件 | 指定記錄檔大小上限(KB)(應用程式) | * 此原則設定可決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，此值預設為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\應用程式\指定記錄檔大小上限(KB) | 啟用，32,768KB |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0243 | Windows元件 | 指定記錄檔大小上限(KB)(應用程式) | * 此原則設定可決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，此值預設為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\應用程式\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 |
| 81 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0245 | Windows元件 | 指定記錄檔大小上限(KB)(安全性) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安全性\指定記錄檔大小上限(KB) | 啟用，81,920KB |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0245 | Windows元件 | 指定記錄檔大小上限(KB)(安全性) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安全性\指定記錄檔大小上限(KB) | 啟用，81,920KB以上 |
| 82 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0246 | Windows元件 | 指定記錄檔大小上限(KB)(安裝) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安裝\指定記錄檔大小上限(KB) | 啟用，32,768KB |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0246 | Windows元件 | 指定記錄檔大小上限(KB)(安裝) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安裝\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 |
| 83 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0248 | Windows元件 | 指定記錄檔大小上限(KB)(系統) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\系統\指定記錄檔大小上限(KB) | 啟用，32,768KB |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0248 | Windows元件 | 指定記錄檔大小上限(KB)(系統) | * 此項原則設定決定記錄檔的大小上限(以KB為單位) * 如果啟用此項原則設定，即可將記錄檔大小上限設定為介於1MB(1,024 KB)至2TB(2,147,483,647 KB)之間(以KB為遞增單位) * 如果停用或未設定此原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更此值，記錄檔大小上限預設值為20MB | 電腦設定\系統管理範本\Windows元件\事件紀錄服務\系統\指定記錄檔大小上限(KB) | 啟用，32,768KB以上 |
| 84 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0252 | Windows元件\遠端桌面服務 | 連線時永遠提示密碼 | * 此項原則設定決定遠端桌面服務是否總是會在連線時，提示用戶端輸入密碼 * 使用者可以使用此項設定，對登入遠端桌面服務的使用者強制執行密碼提示，即使他們已經在遠端桌面連線用戶端中提供過密碼 * 遠端桌面服務預設為允許使用者在遠端桌面連線用戶端中輸入密碼即可自動登入 * 如果此項原則設定為「啟用」，使用者即使已經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。他們會收到要求輸入登入密碼的提示 * 如果此項原則設定為「停用」，使用者只要在遠端桌面連線用戶端中提供過密碼，就一律可以自動登入遠端桌面服務 * 如果此項原則設定為「尚未設定」，則不會於群組原則層級指定自動登入。不過，系統管理員仍然可以使用遠端桌面工作階段主機設定工具，強制執行密碼提示 | 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 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0252 | Windows元件 | 連線時永遠提示密碼 | * 此項原則設定決定遠端桌面服務是否總是會在連線時，提示用戶端輸入密碼 * 使用者可以使用此項設定，對登入遠端桌面服務的使用者強制執行密碼提示，即使他們已經在遠端桌面連線用戶端中提供過密碼 * 遠端桌面服務預設為允許使用者在遠端桌面連線用戶端中輸入密碼即可自動登入 * 如果此項原則設定為「啟用」，使用者即使已經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。他們會收到要求輸入登入密碼的提示 * 如果此項原則設定為「停用」，使用者只要在遠端桌面連線用戶端中提供過密碼，就一律可以自動登入遠端桌面服務 * 如果此項原則設定為「尚未設定」，則不會於群組原則層級指定自動登入。不過，系統管理員仍然可以使用遠端桌面工作階段主機設定工具，強制執行密碼提示 | 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 | 啟用 |
| 85 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0254 | Windows元件 | 為使用中但閒置的遠端桌面服務工作階段設定時間限制 | * 此項原則設定決定使用中的遠端桌面服務工作階段在自動中斷連線之前可以閒置(沒有使用者輸入)的時間上限 * 如果啟用此項原則設定，使用者必須在「閒置工作階段限制」下拉式清單中選取想要的時間限制。經過指定的時間後，遠端桌面服務會自動中斷使用中但閒置之工作階段的連線。使用者會在工作階段中斷連線前兩分鐘收到警告訊息，讓他們可以按下按鍵或移動滑鼠，使工作階段保持使用中狀態。如果使用者有主控台工作階段，則不適用閒置工作階段的時間限制 * 如果停用或未設定此項原則設定，遠端桌面服務會允許工作階段無限期保持使用中但閒置狀態。使用者可以在遠端桌面工作階段主機設定工具的「工作階段」索引標籤上，指定使用中但閒置之工作階段的時間限制 * 如果要在到達時間限制時讓遠端桌面服務終止工作階段而非中斷連線，可以設定「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\超過使用時間限制就終止工作階段」原則設定 * 注意：此項原則設定同時出現在「電腦設定」和「使用者設定」中。如果兩個原則都已設定，「電腦設定」原則具有較高的優先順序 | 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 | 啟用，15分鐘 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0254 | Windows元件 | 為使用中但閒置的遠端桌面服務工作階段設定時間限制 | * 此項原則設定決定使用中的遠端桌面服務工作階段在自動中斷連線之前可以閒置(沒有使用者輸入)的時間上限 * 如果啟用此項原則設定，使用者必須在「閒置工作階段限制」下拉式清單中選取想要的時間限制。經過指定的時間後，遠端桌面服務會自動中斷使用中但閒置之工作階段的連線。使用者會在工作階段中斷連線前兩分鐘收到警告訊息，讓他們可以按下按鍵或移動滑鼠，使工作階段保持使用中狀態。如果使用者有主控台工作階段，則不適用閒置工作階段的時間限制 * 如果停用或未設定此項原則設定，遠端桌面服務會允許工作階段無限期保持使用中但閒置狀態。使用者可以在遠端桌面工作階段主機設定工具的「工作階段」索引標籤上，指定使用中但閒置之工作階段的時間限制 * 如果要在到達時間限制時讓遠端桌面服務終止工作階段而非中斷連線，可以設定「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\超過使用時間限制就結束工作階段」原則設定 * 注意：此項原則設定同時出現在「電腦設定」和「使用者設定」中。如果兩個原則都已設定，「電腦設定」原則具有較高的優先順序 | 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 | 啟用，15分鐘以下，但須大於0分鐘 |
| 86 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0264 | Windows元件 | 設定自動更新 | * 此項原則設定決定這部電腦是否將經由Windows的自動更新服務接收安全性更新和其他重要的下載 * 如果啟用自動更新服務，必須於群組原則設定中選取以下四個選項的其中一個： * 2=下載任何更新前通知我：當Windows找到適用於這部電腦的更新時，狀態列會出現一個帶有訊息的圖示，表示已經準備好下載更新了。按圖示或訊息，提供選項選取特定的更新。Windows然後在背景裡下載所選取的更新。下載完成後，圖示會再次出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 3=(預設設定)自動下載更新，並在準備好安裝更新時通知：Windows找到要套用在電腦上的更新和，以及在背景裡下載這些更新(不通知使用者或插斷此處理)。下載完成後，圖示會出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 4=自動下載更新，並於以下指定的排程安裝更新：使用群組原則設定的選項來指定排程。如果不指定排程的話，所有安裝的預設排程是每天早上3：00。如果有任何更新需要重新開機才能完成安裝的話，Windows將自動重新啟動電腦(如果使用者在Windows準備好重新啟動時登入電腦，使用者將收到通知，並且可以選擇延後重新啟動的時間) | 電腦設定\系統管理範本\Windows元件\Windows Update\設定自動更新 | 啟用，  3-自動下載和通知我安裝 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0264 | Windows元件 | 設定自動更新 | * 此項原則設定決定這部電腦是否將經由Windows的自動更新服務接收安全性更新和其他重要的下載 * 如果啟用自動更新服務，必須於群組原則設定中選取以下四個選項的其中一個： * 2=通知我下載並自動安裝：當Windows找到適用於這部電腦的更新時，狀態列會出現一個帶有訊息的圖示，表示已經準備好下載更新了。按圖示或訊息，提供選項選取特定的更新。Windows然後在背景裡下載所選取的更新。下載完成後，圖示會再次出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 3=自動下載並通知我安裝：(預設設定)Windows找到要套用在電腦上的更新和，以及在背景裡下載這些更新(不通知使用者或插斷此處理)。下載完成後，圖示會出現在狀態列，通知已經準備好安裝更新了。按圖示或訊息，提供選項選取要安裝的更新 * 4=自動下載和排程安裝：使用群組原則設定的選項來指定排程。如果不指定排程的話，所有安裝的預設排程是每天早上3：00。如果有任何更新需要重新開機才能完成安裝的話，Windows將自動重新啟動電腦(如果使用者在Windows準備好重新啟動時登入電腦，使用者將收到通知，並且可以選擇延後重新啟動的時間) | 電腦設定\系統管理範本\Windows元件\Windows Update\設定自動更新 | 啟用，  3-自動下載並通知我安裝 |
| 87 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0270 | Windows元件 | 設定Windows Smart Screen | * 此項原則設定可管理Windows Smart Screen的行為 * Windows Smart Screen會在從網際網路執行無法辨識的程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給Microsoft * 如果啟用此項原則設定，可以透過設定下列其中一個選項來控制Windows Smart Screen的行為： * 在執行不明軟體下載之前需要系統管理員核准 * 在執行不明軟體下載之前警告使用者 * 關閉Smart Screen * 如果停用或未設定此項原則設定，則電腦的系統管理員可以使用「行動作業中心」的「Windows Smart Screen篩選工具設定」管理Windows Smart Screen篩選工具的行為 * 在執行不明軟體下載之前需要系統管理員核准 * 在執行不明軟體下載之前警告使用者 * 關閉Smart Screen篩選工具 | 電腦設定\系統管理範本\Windows元件\檔案總管\設定Windows Smart Screen | 啟用，在執行不明軟體下載之前需要系統管理員核准 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0270 | Windows元件 | 設定Windows Defender SmartScreen | * 此項原則設定可開啟或關閉Windows Defender SmartScreen的行為 * Windows Defender SmartScreen會在從網際網路執行無法辨識的程式或已知有害的應用程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給Microsoft * 如果啟用此項原則設定，將會為所有使用者開啟SmartScreen。可以透過設定下列其中一個選項來控制行為： * 警告並防止略過 * 警告 * 如果使用「警告」選項啟用此原則，SmartScreen對話方塊將警告使用者應用程式看似可疑，但是將允許使用者略過該警告並繼續執行 * 如果使用者告訴SmartScreen執行應用程式，則SmartScreen不會再針對該應用程式警告使用者 * 如果停用此項原則設定，將會為所有使用者關閉SmartScreen。如果使用者嘗試執行來自網際網路的可疑應用程式，將不會收到警告 * 如果未設定此項原則，預設將會啟用SmartScreen，但使用者可變更其設定 | 電腦設定\系統管理範本\Windows元件\檔案總管\設定Windows Defender SmartScreen | 啟用，警告並防止略過 |
| 88 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0287 | Windows元件 | 加入Microsoft地圖 | * 此項原則設定可加入Microsoft地圖。Microsoft地圖是協助使用者選擇如何回應潛在威脅的線上社群。這個社群也可協助停止散佈新惡意軟體的感染 * 可以選擇傳送偵測到之軟體的基本或其他資訊。額外的資訊可協助Microsoft建立新的定義，以協助它保護使用者的電腦。這項資訊可能包含移除有害軟體後，偵測到的項目在使用者電腦上的位置。這個資訊會被自動收集和傳送。在某些情況下，可能會意外將個人資訊傳送給Microsoft。不過，Microsoft不會使用這些資訊來識別使用者的身分或與使用者聯繫 * 可能的選項為： * (0x0)已停用(預設) * (0x1)基本成員資格 * ［(0x2)進階成員資格 * 基本成員資格將會傳送有關偵測到之軟體的基本資訊給Microsoft，包括軟體來源、使用者採取的動作或自動採取的動作，以及這些動作是否成功 * 進階成員資格除了基本資訊之外，還會將更多有關惡意軟體、間諜軟體以及潛在的垃圾軟體的資訊傳送給Microsoft，包括軟體位置、檔案名稱、軟體運作方式，以及使用者對電腦的影響 * 如果啟用此項原則設定，將以指定的成員資格加入Microsoft地圖 * 如果停用或未設定此項原則設定，使用者將不會加入Microsoft地圖 | 電腦設定\系統管理範本\Windows元件\Windows Defender\MAPS\加入Microsoft地圖 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0287 | Windows元件 | 加入Microsoft地圖 | * 此項原則設定可加入Microsoft Active Protection Services(MAPS)，是協助使用者選擇如何回應潛在威脅的線上社群。這個社群也可協助停止散佈新惡意軟體的感染 * 可以選擇傳送偵測到之軟體的基本或其他資訊。額外的資訊可協助Microsoft建立新的安全情報，以協助它保護使用者的電腦。這項資訊可能包含移除有害軟體後，偵測到的項目在使用者電腦上的位置，系統會被自動收集和傳送此資訊。在某些情況下，可能會意外將個人資訊傳送給Microsoft。不過，Microsoft不會使用這些資訊來識別使用者的身分或與使用者聯繫 * 啟用時，此項原則設定將可能傳送給Microsoft之資訊限制為以下設定： * 已停用 * 基本MAPS * 進階MAPS * 基本MAPS將會傳送有關偵測到之軟體的基本資訊給Microsoft，包括軟體來源、使用者採取的動作或自動採取的動作，以及這些動作是否成功 * 進階MAPS除了基本資訊之外，還會將更多有關惡意軟體、間諜軟體以及潛在的垃圾軟體的資訊傳送給Microsoft，包括軟體位置、檔案名稱、軟體運作方式，以及使用者對電腦的影響 * 如果啟用此項原則設定，將以指定的成員資格加入Microsoft MAPS * 如果停用或未設定此項原則設定，使用者將不會加入Microsoft MAPS * 在Windows 10中，基本MAPS已無法使用，因此將值設定為基本MAPS或進階MAPS會將裝置註冊到進階MAPS | 電腦設定\系統管理範本\Windows元件\Windows Defender防毒軟體\MAPS\加入Microsoft地圖 | 啟用：停用 |
| 89 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0289 | Windows元件 | 停用遠端桌面共用 | 停用NetMeeting的遠端桌面共用功能。使用者將無法自遠端進行設定，或者使用這項功能自遠端控制他們的電腦 | 電腦設定\系統管理範本\Windows元件\NetMeeting\停用遠端桌面共用 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0289 | Windows元件 | 停用遠端桌面共用 | * 此項原則設定決定是否禁止使用NetMeeting的遠端桌面共用功能 * 如果啟用此項原則設定，使用者將無法自遠端進行設定，或者使用這項功能自遠端控制他們的電腦 | 電腦設定\系統管理範本\Windows元件\NetMeeting\停用遠端桌面共用 | 啟用 |
| 90 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0293 | Windows元件 | 關閉Microsoft消費者體驗 | * 若啟用此項原則設定，使用者將再也不會看到Microsoft所提供的個人化建議與有關其Microsoft帳戶的通知 * 若停用或未設定此項原則設定，使用者可以看到Microsoft所提供的建議與有關其Microsoft帳戶的通知 | 電腦設定\系統管理範本\Windows元件\雲端內容\關閉Microsoft消費者體驗 | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0293 | Windows元件 | 關閉Microsoft消費者體驗 | * 若啟用此項原則設定，使用者將再也不會看到Microsoft所提供的個人化建議與有關其Microsoft帳戶的通知 * 若停用或未設定此項原則設定，使用者可以看到Microsoft所提供的建議與有關其Microsoft帳戶的通知 * 注意：此設定只適用於Windows10企業版與教育版SKU | 電腦設定\系統管理範本\Windows元件\雲端內容\關閉Microsoft消費者體驗 | 啟用 |
| 91 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0295 | Windows元件 | 使用增強式反詐騙(若可用) | * 此項原則設定決定是否為支援設備配置加強防欺騙功能 * 若未設定此項原則設定，使用者將能夠選擇是否在支援設備上使用加強防欺騙功能 * 若啟用此項原則設定，Windows將要求設備上的所有使用者在支援設備上使用防欺騙功能 * 若停用此項原則設定，設備上的所有使用者都會關閉加強防欺騙功能，並且無法打開此設定 | 電腦設定\系統管理範本\Windows元件\生物識別技術\臉部功能\使用增強式反詐騙(若可用) | 啟用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0295 | Windows元件 | 使用增強式反詐騙 | * 此項原則設定決定是否為Windows Hello臉部驗證使用增強式反詐騙功能 * 若啟用此項原則設定，Windows將要求受管理裝置上的所有使用者為Windows Hello臉部驗證使用增強式反詐騙功能。這會在不支援增強式反詐騙的裝置上停用Windows Hello臉部驗證 * 若停用或未設定此項原則設定，Windows不會要求為Windows Hello臉部驗證使用增強式反詐騙功能 | 電腦設定\系統管理範本\Windows元件\生物識別技術\臉部功能\使用增強式反詐騙 | 啟用 |
| 92 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0297 | Windows元件 | 允許遠端殼層存取 | * 此項原則設定可決定遠端殼層的存取權 * 若啟用此項原則設定，並設定為False，伺服器會拒絕新的遠端殼層連線 * 若停用或未設定此項原則設定，則伺服器會允許新的遠端殼層連線 | 電腦設定\系統管理範本\Windows元件\Windows遠端殼層\允許遠端殼層存取 | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0297 | Windows元件 | 允許遠端殼層存取 | * 此項原則設定可決定遠端殼層的存取權 * 若啟用或未設定此項原則設定，伺服器會接受新的遠端殼層連線 * 若停用此項原則設定，則伺服器會拒絕新的遠端殼層連線 | 電腦設定\系統管理範本\Windows元件\Windows遠端殼層\允許遠端殼層存取 | 停用 |
| 93 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0298 | Windows元件 | 封鎖未受信任的字型 | * 此項原則設定可防止程式載入未受信任的字型。此所稱之未受信任的字型為安裝於%Windir%\Fonts目錄外之任何字型 * 此項原則有三種設定：開啟、關閉和稽核。預設為關閉，不會封鎖字型 * 如果還沒準備好在機關中部署這項功能，您可以使用「稽核」模式查看封鎖未受信任的字型是否會產生任何相容性之問題 | 電腦設定\系統管理範本\系統\緩和選項\封鎖未受信任的字型 | 啟用，封鎖未受信任的字型並紀錄 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0298 | 系統\緩和選項 | 封鎖未受信任的字型 | * 此項原則設定決定是否防止程式載入未受信任的字型 * 未受信任的字型為安裝於%Windir%\Fonts目錄外之任何字型。此功能有3種選項： * 封鎖未受信任的字型並記錄事件 * 不封鎖未受信任的字型 * 記錄事件，而不封鎖未受信任的字型 * 如果還沒準備好在機關中部署這項功能，可以使用「記錄事件，而不封鎖未受信任的字型」模式，查看封鎖未受信任的字型是否會產生任何相容性之問題 | 電腦設定\系統管理範本\系統\緩和選項\封鎖未受信任的字型 | 啟用，封鎖未受信任的字型並紀錄 |
| 94 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0299 | Windows元件 | 支援使用憑證進行裝置驗證 | * 要支援裝置使用憑證驗證，裝置帳戶網域需要支援使用憑證進行電腦帳戶驗證，並需要可連線至網域控制站(DC)的能力 * 此項原則設定可讓使用者設定Kerberos支援嘗試使用裝置的憑證驗證到網域 * 若啟用此項原則設定，裝置憑證將根據下列選項選取： * 自動：裝置將嘗試使用本身的憑證驗證。如果網域控制站(DC)不支援使用憑證進行電腦帳戶驗證，則會嘗試使用密碼驗證 * 強制：裝置將總是使用本身的憑證驗證。如果找不到支援使用憑證進行電腦帳戶驗證的網域控制站(DC)，則驗證會失敗 * 若未設定此項原則設定，可使用「自動」 | 電腦設定\系統管理範本\系統\Kerberos\支援使用憑證進行裝置驗證 | 啟用-自動 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0299 | 系統\Kerberos | 支援使用憑證進行裝置驗證 | * 要支援裝置使用憑證驗證，裝置帳戶網域需要支援使用憑證進行電腦帳戶驗證，並需要可連線至網域控制站(DC)的能力 * 此項原則設定可讓使用者設定Kerberos支援嘗試使用裝置的憑證驗證到網域 * 若啟用此項原則設定，裝置憑證將根據下列選項選取： * 自動：裝置將嘗試使用本身的憑證驗證。如果網域控制站(DC)不支援使用憑證進行電腦帳戶驗證，則會嘗試使用密碼驗證 * 強制：裝置將總是使用本身的憑證驗證。如果找不到支援使用憑證進行電腦帳戶驗證的網域控制站(DC)，則驗證會失敗 * 若未設定此項原則設定，可使用「自動」 | 電腦設定\系統管理範本\系統\Kerberos\支援使用憑證進行裝置驗證 | 啟用-自動 |
| 95 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0300 | 印表機 | 擴充指向並列印連線以搜尋Windows Update | * 此項原則設定決定可讓使用者管理用戶端電腦在何處搜尋指向並列印驅動程式 * 如果啟用此項原則設定，用戶端電腦在本機驅動程式存放區與伺服器驅動程式快取中找不到相容驅動程式後，會繼續從Windows Update搜尋相容的指向並列印驅動程式 * 如果停用此項原則設定，用戶端電腦只會在本機驅動程式存放區和伺服器驅動程式快取中搜尋相容的指向並列印驅動程式。如果找不到相容驅動程式，則指向並列印連線會失敗 | 電腦設定\系統管理範本\印表機\擴充指向並列印連線以搜尋Windows Update | 停用 |
| 修改後 | Windows10 Computer Settings | TWGCB-01-005-0300 | 印表機 | 擴充指向並列印連線以搜尋Windows Update | * 此項原則設定決定可讓使用者管理用戶端電腦在何處搜尋指向並列印驅動程式 * 如果啟用此項原則設定，用戶端電腦在本機驅動程式存放區與伺服器驅動程式快取中找不到相容驅動程式後，會繼續從Windows Update搜尋相容的指向並列印驅動程式 * 如果停用此項原則設定，用戶端電腦只會在本機驅動程式存放區和伺服器驅動程式快取中搜尋相容的指向並列印驅動程式。如果找不到相容驅動程式，則指向並列印連線會失敗 * 如果未設定此項原則設定，其行為須視所使用的Windows版本而定。根據預設，Windows旗艦版、專業版及家用SKU版會視需求從Windows Update搜尋相容的指向並列印驅動程式。然而，如果使用其他Windows版本，如Windows企業版、所有的Windows Server 2008 R2及更新版本)，就必須明確啟用此項原則設定才會有相同的行為 | 電腦設定\系統管理範本\印表機\擴充指向並列印連線以搜尋Windows Update | 停用 |
| 96 | 修改前 | Windows10 User Settings | TWGCB-01-005-0308 | 個人化 | 螢幕保護裝置逾時 | * 此項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動 * 如果已設定，這個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。如果設為零，螢幕保護裝置將不會啟動 * 在下列任一狀況下，此項設定沒有作用： * 設定已停用或未設定 * 等候時間設為零 * 「啟用螢幕保護裝置」設定已停用 * 「螢幕保護裝置執行檔名稱」設定和用戶端電腦的「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊都沒有在用戶端上指定有效的現有螢幕保護裝置程式 * 如果未設定，則會使用透過「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊在用戶端上設定的等候時間。預設值是15分鐘 | 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 | 啟用，900秒 |
| 修改後 | Windows10 User Settings | TWGCB-01-005-0308 | 個人化 | 螢幕保護裝置逾時 | * 此項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動 * 如果已設定，這個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。如果設為零，螢幕保護裝置將不會啟動 * 在下列任一狀況下，此項設定沒有作用： * 設定已停用或未設定 * 等候時間設為零 * 「啟用螢幕保護裝置」設定已停用 * 「螢幕保護裝置執行檔名稱」設定和用戶端電腦的「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊都沒有在用戶端上指定有效的現有螢幕保護裝置程式 * 如果未設定，則會使用透過「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊在用戶端上設定的等候時間。預設值是15分鐘 | 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 | 啟用，900秒以下，但須大於0秒 |
| 97 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0313 | 具有進階安全性的Windows防火牆 | Windows防火牆：禁止通知(網域) | * 此項原則設定決定當程式要求Windows防火牆將程式新增到程式例外清單時，是否禁止Windows防火牆對使用者顯示通知 * 如果啟用此項原則設定，Windows防火牆將禁止顯示這些通知 * 如果停用此項原則設定，Windows防火牆就會允許顯示這些通知。在「控制台」的「Windows防火牆」元件中，「當Windows防火牆封鎖新的程式時請通知我」核取方塊將設定為選取狀態，且系統管理員無法將其清除 * 如果未設定此項原則設定，Windows防火牆會當作已停用此項原則設定，在「控制台」的「Windows防火牆」元件中，「當Windows防火牆封鎖新的程式時請通知我」核取方塊仍預設為選取狀態，但系統管理員可進行變更 | 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 | 停用 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0313 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：顯示通知 | * 此項原則設定決定當程式要求Windows Defender防火牆將程式新增到程式例外清單時，是否禁止Windows Defender防火牆對使用者顯示通知 * 如果此項原則設定為「否」，Windows Defender防火牆將禁止顯示這些通知 * 如果此項原則設定為「是」，Windows Defender防火牆就會允許顯示這些通知。在「控制台」的「Windows Defender防火牆」元件中，「當Windows Defender防火牆封鎖新的程式時請通知我」核取方塊將設定為選取狀態，且系統管理員無法將其清除 * 如果未設定此項原則設定，Windows Defender防火牆會當作已停用此項原則設定，在「控制台」的「Windows Defender防火牆」元件中，「當Windows Defender防火牆封鎖新的程式時請通知我」核取方塊仍預設為選取狀態，但系統管理員可進行變更 | 電腦設定\ Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\顯示通知 | 是 |
| 98 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0314 | 具有進階安全性的Windows防火牆 | Windows防火牆：禁止單點傳送回應到多點傳送或廣播要求(網域) | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果啟用此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果停用或未設定此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 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 | 啟用 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0314 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：允許單點傳播回應 | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\ Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\允許單點傳播回應 | 否 |
| 99 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0315 | 具有進階安全性的Windows防火牆 | 套用本機防火牆規則(網域) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 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 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0315 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\套用本機防火牆規則 | 否 |
| 100 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0316 | 具有進階安全性的Windows防火牆 | 套用本機連線安全性規則(網域) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 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 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0316 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\設定\套用本機連線安全性規則 | 否 |
| 101 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0317 | 具有進階安全性的Windows防火牆 | 輸出連線(網域) | 此項原則設定決定Windows防火牆對於輸出連線的預設行為 | 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 | 允許(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0317 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\輸出連線 | 允許(預設) |
| 102 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0318 | 具有進階安全性的Windows防火牆 | 輸入連線(網域) | 此項原則設定決定Windows防火牆對於輸入連線的預設行為 | 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 | 封鎖(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0318 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\輸入連線 | 封鎖(預設) |
| 103 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0319 | 具有進階安全性的Windows防火牆 | 記錄丟棄的封包(網域) | 此項原則設定決定Windows防火牆是否記錄丟棄的封包 | 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 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0319 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\記錄丟棄的封包 | 是 |
| 104 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0320 | 具有進階安全性的Windows防火牆 | 記錄成功的連線(網域) | 此項原則設定決定Windows防火牆是否記錄成功的連線 | 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 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0320 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\記錄成功的連線 | 是 |
| 105 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0321 | 具有進階安全性的Windows防火牆 | 大小限制(網域) | 此項原則設定決定Windows防火牆記綠檔的大小 | 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 | 16,384 KB |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0321 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\大小限制 | 16,384 KB以上 |
| 106 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0322 | 具有進階安全性的Windows防火牆 | 名稱(網域) | 此項原則設定決定Windows防火牆記綠檔的名稱 | 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 | %windir%\system32\logfiles\firewall\domainfirewall.log |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0322 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\記錄\名稱 | %windir%\system32\logfiles\firewall\domainfirewall.log |
| 107 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0323 | 具有進階安全性的Windows防火牆 | 防火牆狀態(網域) | * 此項原則設定決定是否開啟Windows防火牆 | 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\防火牆狀態 | 開啟(建議選項) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0323 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：網域設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\網域設定檔\防火牆狀態 | 開啟(建議選項) |
| 108 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0324 | 具有進階安全性的Windows防火牆 | 顯示通知(私人) | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 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\私人設定檔\自訂\防火牆設定\顯示通知 | 是(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0324 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：顯示通知 | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\顯示通知 | 是 |
| 109 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0325 | 具有進階安全性的Windows防火牆 | 允許單點傳播回應(私人) | * 此項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果啟用此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果停用或未設定此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效Windows防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 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\私人設定檔\自訂\單點傳播回應\允許單點傳播回應 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0325 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：允許單點傳播回應 | * 此項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\允許單點傳播回應 | 否 |
| 110 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0326 | 具有進階安全性的Windows防火牆 | 套用本機防火牆規則(私人) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 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\私人設定檔\自訂\規則合併\套用本機防火牆規則 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0326 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\套用本機防火牆規則 | 否 |
| 111 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0327 | 具有進階安全性的Windows防火牆 | 套用本機連線安全性規則(私人) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 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\私人設定檔\自訂\規則合併\套用本機連線安全性規則 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0327 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\設定\套用本機連線安全性規則 | 否 |
| 112 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0328 | 具有進階安全性的Windows防火牆 | 防火牆狀態(私人) | 此項原則設定決定是否開啟Windows防火牆 | 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\私人設定檔\防火牆狀態 | 開啟(建議選項) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0328 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\防火牆狀態 | 開啟(建議選項) |
| 113 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0329 | 具有進階安全性的Windows防火牆 | 輸出連線(私人) | 此項原則設定決定Windows防火牆對於輸出連線的預設行為 | 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\私人設定檔\輸出連線 | 允許(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0329 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\輸出連線 | 允許(預設) |
| 114 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0330 | 具有進階安全性的Windows防火牆 | 輸入連線(私人) | 此項原則設定決定Windows防火牆對於輸入連線的預設行為 | 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\私人設定檔\輸入連線 | 封鎖(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0330 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\輸入連線 | 封鎖(預設) |
| 115 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0331 | 具有進階安全性的Windows防火牆 | 名稱(私人) | 此項原則設定決定Windows防火牆記綠檔的名稱 | 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\私人設定檔\記錄\名稱 | %windir%\System32\LogFiles\Firewall\privatefirewall.log |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0331 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\名稱 | %windir%\System32\LogFiles\Firewall\privatefirewall.log |
| 116 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0332 | 具有進階安全性的Windows防火牆 | 大小限制(私人) | 此項原則設定決定Windows防火牆記綠檔的大小 | 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\私人設定檔\記錄\大小限制 | 16,384 KB |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0332 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\大小限制 | 16,384 KB以上 |
| 117 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0333 | 具有進階安全性的Windows防火牆 | 記錄丟棄的封包(私人) | 此項原則設定決定Windows防火牆是否記錄丟棄的封包 | 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\私人設定檔\記錄\記錄丟棄的封包 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0333 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\記錄丟棄的封包 | 是 |
| 118 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0334 | 具有進階安全性的Windows防火牆 | 記錄成功的連線(私人) | 此項原則設定決定Windows防火牆是否記錄成功的連線 | 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\私人設定檔\記錄\記錄成功的連線 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0334 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：私人設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\私人設定檔\記錄\記錄成功的連線 | 是 |
| 119 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0335 | 具有進階安全性的Windows防火牆 | 顯示通知(公用) | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 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\公用設定檔\自訂\防火牆設定\顯示通知 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0335 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：顯示通知 | 此項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\顯示通知 | 是 |
| 120 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0336 | 具有進階安全性的Windows防火牆 | 允許單點傳播回應(公用) | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果啟用此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果停用或未設定此項原則設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 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\公用設定檔\自訂\單點傳播回應\允許單點傳播回應 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0336 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：允許單點傳播回應 | * 此項原則設定決定是否禁止此電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 * 如果此項原則設定為「是」，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會封鎖由其他電腦傳送的單點傳送回應 * 如果此項原則設定設定為「否」或未設定，且這部電腦將多點傳送或廣播訊息傳送到其他電腦，則Windows Defender防火牆會等候來自其他電腦的單點傳送回應3秒鐘，然後就會封鎖所有回應 * 注意：如果單點傳送訊息為此電腦傳送之「動態主機設定通訊協定(DHCP)」廣播訊息的回應，則此原則設定無效。Windows Defender防火牆會永遠允許那些DHCP單點傳送回應。但是此原則設定可能會干擾偵測名稱衝突的NetBIOS訊息 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\允許單點傳播回應 | 否 |
| 121 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0337 | 具有進階安全性的Windows防火牆 | 套用本機防火牆規則(公用) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 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\公用設定檔\自訂\規則合併\套用本機防火牆規則 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0337 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：套用本機防火牆規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\套用本機防火牆規則 | 否 |
| 122 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0338 | 具有進階安全性的Windows防火牆 | 套用本機連線安全性規則(公用) | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 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\公用設定檔\自訂\規則合併\套用本機連線安全性規則 | 否 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0338 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：套用本機連線安全性規則 | 此項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\設定\套用本機連線安全性規則 | 否 |
| 123 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0339 | 具有進階安全性的Windows防火牆 | 防火牆狀態(公用) | 此項原則設定決定是否開啟Windows防火牆 | 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\公用設定檔\防火牆狀態 | 開啟(建議選項) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0339 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：防火牆狀態 | 此項原則設定決定是否開啟Windows Defender防火牆 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\防火牆狀態 | 開啟(建議選項) |
| 124 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0340 | 具有進階安全性的Windows防火牆 | 輸出連線(公用) | 此項原則設定決定Windows防火牆對於輸出連線的預設行為 | 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\公用設定檔\輸出連線 | 允許(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0340 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：輸出連線 | 此項原則設定決定Windows Defender防火牆對於輸出連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\輸出連線 | 允許(預設) |
| 125 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0341 | 具有進階安全性的Windows防火牆 | 輸入連線(公用) | 此項原則設定決定Windows防火牆對於輸入連線的預設行為 | 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\公用設定檔\輸入連線 | 封鎖(預設) |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0341 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：輸入連線 | 此項原則設定決定Windows Defender防火牆對於輸入連線的預設行為 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\輸入連線 | 封鎖(預設) |
| 126 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0342 | 具有進階安全性的Windows防火牆 | 大小限制(公用) | 此項原則設定決定Windows防火牆記綠檔的大小 | 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\公用設定檔\記錄\大小限制 | 16384 KB |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0342 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：大小限制 | 此項原則設定決定Windows Defender防火牆記綠檔的大小 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\大小限制 | 16,384 KB以上 |
| 127 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0343 | 具有進階安全性的Windows防火牆 | 記錄丟棄的封包(公用) | 此項原則設定決定Windows防火牆是否記錄丟棄的封包 | 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\公用設定檔\記錄\記錄丟棄的封包 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0343 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：記錄丟棄的封包 | 此項原則設定決定Windows Defender防火牆是否記錄丟棄的封包 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\記錄丟棄的封包 | 是 |
| 128 | 修改前 | Windows10 Firewall Settings | TWGCB-01-005-0344 | 具有進階安全性的Windows防火牆 | 記錄成功的連線(公用) | 此項原則設定決定Windows防火牆是否記錄成功的連線 | 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\公用設定檔\記錄\記錄成功的連線 | 是 |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0344 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：記錄成功的連線 | 此項原則設定決定Windows Defender防火牆是否記錄成功的連線 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\記錄成功的連線 | 是 |
| 129 | 修改前 | Windows10 Computer Settings | TWGCB-01-005-0345 | 具有進階安全性的Windows防火牆 | 名稱(公用) | 此項原則設定決定Windows防火牆記綠檔的名稱 | 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\公用設定檔\記錄\名稱 | %windir%\system32\logfiles\firewall\publicfirewall.log |
| 修改後 | Windows10 Firewall Settings | TWGCB-01-005-0345 | 具有進階安全性的Windows防火牆 | Windows Defender防火牆：公用設定檔：名稱 | 此項原則設定決定Windows Defender防火牆記綠檔的名稱 | 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows Defender防火牆\具有進階安全性的Windows Defender防火牆\內容\公用設定檔\記錄\名稱 | %windir%\system32\logfiles\firewall\publicfirewall.log |
| 本中心整理 | | | | | | | | |