政府組態基準

Microsoft Windows 8.1

TWGCB-01-004

(V1.7)

行政院國家資通安全會報技術服務中心

中華民國111年1月

修訂歷史紀錄表

項次	版次	修訂日期	說 明
1	1.0	105/3/23	新編
2	1.1	105/10/25	▪修改表 1 Windows8.1 Computer Settings 之項數與合計 ▪移除表 2 項次共 6 項(原項次 10、11、12、13、115 及 116) ▪修改表 2 項次 173、175、178 之 GCB 說明 ▪修改表 2 項次 2 之「密碼最長使用期限」設定值，由「60 天」調整為「90 天以下」 ▪修改表 2 項次 3 之「最小密碼長度」設定值，由「12 個字元」調整為「8 個字元以上」 ▪修改表 2 項次 5 之「強制執行密碼歷程記錄」設定值，由「24 記憶的密碼」調整為「3 以上記憶的密碼」
3	1.2	105/12/2	▪文件封面「國家資通安全科技中心」改為「行政院國家資通安全會報技術服務中心」 ▪新增「備註」欄位 ▪恢復表 2 項次共 6 項(原 1.0 版文件項次 10、11、12、13、115 及 116) ，並新增備註說明「於 105 年刪除此設定條目」 ▪新增表 2 項次 2「密碼最長使用期限」之備註「原設定值為 60 天，修訂為 90 天以下」 ▪新增表 2 項次 3「最小密碼長度」之備註「原設定值為 12 個字元，修訂為 8 個字元以上」 ▪新增表 2 項次 5「強制執行密碼歷程記錄」之備註「原設定值為 24 記憶的密碼，修訂為 3 以上記憶的密碼」
4	1.3	106/3/15	▪修改表 2 項次 107 之「網域成員：安全通道資料加以數位簽章(可能的話)」調整為「網域成員：安全

項次	版次	修訂日期	說 明
			通道資料加以數位簽章(自動)」
5	1.4	107/1/29	▪修改表 2 項次 167 之「關機：清除虛擬記憶體分頁檔」GPO 設定路徑，由「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」調整為「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」 ▪修改表 2 項次 173 之「使用者帳戶控制：在管理員核准模式，系統管理員之提升權限提示的行為」設定值，由「提示要求同意」調整為「在安全桌面提示要求同意」 ▪修改表 2 項次 197 之「拒絕以服務方式登入」設定值，由「No One」調整為「Guests」 ▪修改表 2 項次 195 之「拒絕從網路存取這台電腦」設定值，由「Guests」調整為「NT AUTHORITY\Local Account, Guests」 ▪修改表 2 項次 199 之「拒絕透過遠端桌面服務登入」設定值，由「Guests」調整為「NT AUTHORITY\Local Account, Guests」 ▪調整表 2 項次 257 之「設定用戶端連線加密層級」設定值，由「啟用」調整為「啟用，高等級」
6	1.5	108/12/17	▪移除「CCE-ID」欄位，將 CCE-ID 資料移至「備註」欄位 ▪新增「TWGCB-ID」欄位與資料，並調整順序
7	1.6	108/2/20	▪修改表 2 項次 20 之原則設定名稱，由「6to4 狀態」調整為「設定 6to4 狀態」 ▪修改表 2 項次 21 之原則設定名稱，由「IP-HTTPS 狀態」調整為「設定 IP-HTTPS 狀態」 ▪修改表 2 項次 22 之原則設定名稱，由「ISATAP 狀

項次	版次	修訂日期	說 明
			態」調整為「設定 ISATAP 狀態」 ▪ 修改表 2 項次 23 之原則設定名稱，由「Teredo 狀態」調整為「設定 Teredo 狀態」 ▪ 修改表 2 項次 29 之原則設定名稱，由「登錄原則處理」調整為「設定登錄原則處理」 ▪ 修改表 2 項次 230 之原則設定名稱，由「關閉 Windows Mail 應用程式」調整為「關閉 Windows 郵件應用程式」 ▪ 修改表 2 項次 230 與 231 之 GPO 設定路徑，由「電腦設定\系統管理範本\Windows 元件\Windows Mail\」調整為「電腦設定\系統管理範本\Windows 元件\Windows 郵件\」
8	1.7	111/1/4	▪ 封面新增「TWGCB-ID」文件編號 ▪ 刪除 6 項設定項目，異動內容詳見附件 1

目次

表目次

壹、 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。

一、適用環境

本文件適用於微軟公司所發行之 Windows 8.1 作業系統。

二、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 8.1 組態基準計有 334 項設定項目，項目統計詳見表 1。

表1　Windows 8.1 組態基準項目統計

項次	項目	項數	合計
1	Windows8.1 Account Settings	9	334
2	Windows8.1 Computer Settings	279	
3	Windows8.1 User Settings	13	
4	Windows8.1 Firewall Settings	33	

資料來源：本中心整理

三、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。

貳、 Windows 8.1 政府組態基準列表

表2　Windows 8.1 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
1	Windows8.1 Account Settings	TWGCB-01-004-0001	帳戶原則\密碼原則	密碼最短使用期限	▪密碼最短使用期限這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	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-35366-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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			
2	Windows8.1 Account Settings	TWGCB-01-004-000	帳戶原則\密碼原則	密碼最長使用期限	▪這項安全性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	電腦設定\Windows 設定\安全性設定\帳	90 天以下	▪原設定值為「60 天」，修訂

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		2			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	戶原則\密碼原則\密碼最長使用期限		為「90 天以下」 ▪ CCE-ID：CCE-34907-6
3	Windows8.1	TWGC	帳戶原	最小密碼	▪ 此項安全性設定決定使用者帳	電腦設定	8 個字元	▪ 原設定值

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Account Settings	B-01-004-0003	則\密碼原則	長度	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	\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	以上	為「12 個字元」，修訂為「8 個字元以上」 ▪CCE-ID：CCE-33789-9
4	Windows8.1 Account Settings	TWGCB-01-004-0004	帳戶原則\密碼原則	密碼必須符合複雜性需求	▪這項安全性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： -英文大寫字元(A 到 Z)	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-33777-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-英文小寫字元(a 到 z) -10 進位數字(0 到 9) -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			
5	Windows8.1 Account Settings	TWGCB-01-004-0005	帳戶原則\密碼原則	強制執行密碼歷程記錄	▪這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 ▪這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	▪原設定值為「24 記憶的密碼」，修訂為「3 以上記憶的密碼」 ▪CCE-ID：CCE-35219-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
6	Windows8.1 Account Settings	TWGCB-01-004-0006	帳戶原則\密碼原則	使用可還原的加密來存放密碼	▪ 這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，否則絕不應該啟用這項原則 ▪ 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，便需要這項原則。在網際網路資訊服務	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-35370-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(IIS)中使用摘要式驗證時，也需要這項原則			
7	Windows8.1 Account Settings	TWGCB-01-004-0007	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	CCE-ID：CCE-33728-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
8	Windows8.1 Account Settings	TWGCB-01-004-0008	帳戶原則\帳戶原則	重設帳戶鎖定計數器的時間間隔	▪此安全性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	CCE-ID：CCE-35408-4
9	Windows8.1 Account Settings	TWGCB-01-004-0009	帳戶原則\帳戶原則	帳戶鎖定期間	▪這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	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	CCE-ID：CCE-35409-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					戶鎖定期間必須大於或等於重設時間			
10	Windows8.1 Computer Settings	TWGCB-01-004-0010	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 ▪如果啟用這個設定，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-35799-6
11	Windows8.1 Computer Settings	TWGCB-01-004-0011	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	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-35800-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					映 ▪如果啟用這個設定，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			
12	Windows8.1 Computer Settings	TWGCB-01-004-0012	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	▪這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 ▪如果啟用這項原則設定，網域使用者在設定網路的位置時必須提升權限 ▪如果停用或未設定這項原則設定，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-35554-5
13	Windows8.1 Computer	TWGCB-01-0	網路\網路連	禁止在您的 DNS	▪這項原則設定決定使用者是否可以安裝及設定網路橋接器	電腦設定\系統管理範本\網路\	啟用	CCE-ID：CCE-33107-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0013	線	網域網路上安裝、設定及使用網路橋接	▪注意：這個設定與位置有關。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，才會套用這個設定 ▪如果設定更新之後，電腦又連線到其他不同的 DNS 網域網路，這個設定將不會生效，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 ▪如果停用或沒有進行此設定，則使用者可以建立並修改網路橋接器的設定。啟用這個設定並不會從使用者的電腦移除現	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		4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					存的網路橋接器			
14	Windows8.1 Computer Settings	TWGCB-01-004-0014	網路\網路連線	透過內部網路路由傳送所有流量	▪這個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 ▪如果啟用這個原則設定，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 ▪如果停用這個原則設定，執行	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-35561-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果未設定這個原則設定，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			
15	Windows8.1 Computer Settings	TWGCB-01-004-0015	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	▪ 這個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，當這個原則設定值是[未設定]時，預設為啟用 ▪ 如果啟用這個原則設定，當電腦至少有一個使用中的網際網路連線時，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	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	CCE-ID：CCE-35242-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					連線時，也會封鎖相同 Windows 網域的新自動連線。這個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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用這個原則設定，則允許多個網際網路、Windows 網域或兩者的同時連線 ▪如果這個原則設定值是[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			
16	Windows8.1 Computer Settings	TWGCB-01-004-001	網路\Windows 連線	當連線到通過網域驗證的網	▪這個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	電腦設定\系統管理範本\網路\Windows 連線	啟用	CCE-ID：CCE-35375-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		6	管理員	路時，禁止連線到非網域網路	▪如果啟用這個原則設定，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 -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 -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 -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這個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	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		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					手動連線 -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這個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			
17	Windows8.1 Computer Settings	TWGCB-01-004-0017	網路\連結階層拓樸搜尋	開啟 Mapper I/O(LLTDIO)驅動程式	▪這個原則設定會變更 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 ▪如果啟用這個原則設定，使用	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	CCE-ID：CCE-34262-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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] ▪ 如果停用或未設定這個原則設定，將套用 LLTDIO 的預設行為			
18	Windows8.1 Computer Settings	TWGCB-01-004-0018	網路\連結階層拓樸搜尋	開啟 Responder(RSPNDR)驅動程式	▪ 這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	電腦設定\系統管理範本\網路\連結階層拓樸搜尋\開啟 Responder(RSP	停用	CCE-ID：CCE-34073-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果啟用這項原則設定，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」 ▪ 如果停用或未設定這項原則設定，將套用 Responder 的預設行為	NDR)驅動程式		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
19	Windows8.1 Computer Settings	TWGCB-01-004-0019	網路\Microsoft 對等網路服務	關閉 Microsoft 對等網路服務	▪ 這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 ▪ 如果啟用此設定，將會關閉對等通訊協定 ▪ 如果停用或沒有進行此設定，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-33208-0
20	Windows8.1 Computer Settings	TWGCB-01-004-0020	網路\TCP 設定值	設定 6to4 狀態	▪ 這個原則設定可設定 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：	電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術\設定 6to4 狀態	啟用	CCE-ID：CCE-33215-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用或未設定這個原則設定，則使用本機主機設定。 ▪ 如果啟用這個原則設定，可在 6to4 指定以下其中一項設定： (1)原則預設狀態：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 (2)原則啟用狀態：如果有全域			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (3)原則停用狀態：6to4 為關閉狀態，而且無法使用與 6to4 的連線			
21	Windows8.1 Computer Settings	TWGCB-01-004-0021	網路\TCPIP 設定值	設定 IP-HTTPS 狀態	▪ 這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 ▪ 如果停用或未設定這項原則設定，則使用本機主機設定 ▪ 如果啟用這項原則設定，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： (1)原則預設狀態：沒有其他連	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-34036-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					線選項時即使用 IP-HTTPS 介面 (2)原則啟用狀態：即使主機有其他連線介面，仍會一直提供 IP-HTTPS 介面 (3)原則停用狀態：主機不提供 IP-HTTPS 介面			
22	Windows8.1 Computer Settings	TWGCB-01-0004-0022	網路\TCP 設定值\IPv6 轉換技術	設定 ISATAP 狀態	▪這項原則設定可設定「內部網站自動通道定址通訊協定」(Intra-SiteAutomaticTunnelAddressingProtocol，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 ▪如果停用或未設定這項原則設	電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術\設定 ISATAP 狀態	啟用	CCE-ID：CCE-34389-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定，則使用本機主機設定 ▪ 如果啟用這項原則設定，可以下列其中一個設定來設定 ISATAP： (1)原則預設狀態：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 (2)原則啟用狀態：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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (3)原則停用狀態：主機不提供 ISATAP 介面			
23	Windows8.1 Computer Settings	TWGCB-01-0004-0023	網路\TCP 設定值\IPv6 轉換技術	設定 Teredo 狀態	▪ 這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 ▪ 如果停用或未設定這項原則設定，則使用本機主機設定 ▪ 如果啟用這項原則設定，可用下列其中一個設定來設定 Teredo： (1)預設值：預設狀態是「用戶	電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術\設定 Teredo 狀態	啟用	CCE-ID：CCE-33577-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					端」 (2)停用：主機不提供 Teredo 介面 (3)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 (4)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			
24	Windows8.1 Computer Settings	TWGCB-01-004-0024	網路\Windows Connect Now	使用 Windows Connect Now 進行無線設定	▪這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	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-34326-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					媒體上進行搜索與設定 ▪如果啟用這項原則設定，就有額外選項可以關閉特定媒體上的操作 ▪如果停用此原則設定，將會停用所有媒體上的操作。如果未設定此原則設定，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			
25	Windows8.1 Computer Settings	TWGCB-01-004-0025	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	電腦設定\系統管理範本\網路\Windows Connect Now\禁止存取 Windows Connect Now	啟用	CCE-ID：CCE-35606-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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	精靈		
26	Windows8.1 Computer Settings	TWGCB-01-004-0026	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	▪這個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]原則後才能套用這個設定。如果啟用這個原則設定，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	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-35802-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用或未設定這個原則設定，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：如果啟用這個原則設定，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			
27	Windows8.1 Computer Settings	TWGCB-01-004-002	系統\裝置安裝	防止從網際網路擷取裝置中	▪ 這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	電腦設定\系統管理範本\系統\裝置安裝\防止	啟用	CCE-ID：CCE-35171-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		7		繼資料	▪如果啟用這項原則設定，Windows 不會從網際網路為安裝的裝置擷取裝置中繼資料。這項原則設定會覆寫「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 ▪如果停用或未設定這項原則設定，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	從網際網路擷取裝置中繼資料		
28	Windows8.1 Computer Settings	TWGCB-01-004-0028	系統\開機初期的反惡意程	開機啟動驅動程式初始化原則	▪這個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	電腦設定\系統管理範本\系統\開機初期的反惡意程式碼\開	啟用-良好與不明	CCE-ID：CCE-33231-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			式碼		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，但為開機所需：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	機啟動驅動程式初始化原則		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，便會初始化判斷為[良好]、[不明]或[不良，但為開機關鍵]的開機啟動驅動程式，但不會初始判斷為[不良]的驅動程式 ▪如果的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，則這個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			
29	Windows8.1	TWGC	系統\	設定登錄	▪這項原則設定可決定更新登錄	電腦設定\系統	啟用-	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0029	群組原則	原則處理	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 ▪ 如果啟用這項原則設定，可以使用所提供的核取方塊來變更選項 ▪ 如果停用這項原則、或不加以設定，它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	管理範本\系統\群組原則\設定登錄原則處理	即使群組原則物件尚未變更也進行處理	CCE-35384-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
30	Windows8.1 Computer Settings	TWGCB-01-004-0030	系統\登入	不要顯示網路選取 UI	▪ 這個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 ▪ 如果啟用這個原則設定，則登入 Windows 之後才能變更電腦的網路連線狀態 ▪ 如果停用或未設定這個原則設定，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	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-33822-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					路			
31	Windows8.1 Computer Settings	TWGCB-01-004-0031	系統\登入	不要列舉加入網域電腦上的連線使用者	▪這個原則設定會禁止列舉加入網域電腦上的連線使用者 ▪如果啟用這個原則設定，登入介面不會列舉加入網域電腦上的連線使用者 ▪如果停用或未設定這個原則設定，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-35207-0
32	Windows8.1 Computer Settings	TWGCB-01-004-0032	系統\登入	不要處理只執行一次清單	▪這個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	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-34705-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					標準清單中 ▪如果啟用這個原則設定，則系統會略過執行一次清單 ▪如果停用或未設定這個原則設定，系統會執行只執行一次清單中的程式 ▪這個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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					中。另請參閱[不要處理舊版執行清單]原則設定			
33	Windows8.1 Computer Settings	TWGCB-01-004-0033	系統\登入	列舉加入網域電腦上的本機使用者	▪這個原則設定會允許列舉加入網域電腦上的本機使用者 ▪如果啟用這個原則設定，登入介面將會列舉加入網域電腦上的本機使用者 ▪如果停用或未設定這個原則設定，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-34838-3
34	Windows8.1 Computer Settings	TWGCB-01-004-0034	系統\登入	關閉鎖定畫面上的應用程式通知	▪這個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	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-34837-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用或未設定這個原則設定，則使用者可以選擇要在鎖定畫面上顯示通知的應用程式			
35	Windows8.1 Computer Settings	TWGCB-01-004-0035	系統\登入	開啟 PIN 登入	▪這個原則設定可以讓使用者控制是否讓網域使用者使用 PIN 登入 ▪如果啟用這個原則設定，網域使用者可以設定並使用 PIN 登入 ▪如果停用或未設定這個原則設定，則網域使用者無法設定並使用 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 PIN 登入	停用	CCE-ID：CCE-35095-9
36	Windows8.1	TWGC	系統\	永遠使用	▪這項原則設定決定是否強制使	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0036	登入	傳統登入	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。這個設定只能在電腦未加入網域時使用	管理範本\系統\登入\永遠使用傳統登入		CCE-33513-3
37	Windows8.1 Computer Settings	TWGCB-01-004-0037	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)	▪ 這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 ▪ 如果啟用或沒有設定此原則，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-33782-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
38	Windows8.1 Computer Settings	TWGCB-01-004-0038	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)	▪這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 ▪如果啟用或沒有設定此原則，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-35462-1
39	Windows8.1 Computer Settings	TWGCB-01-004-0039	系統\遠端協助	設定提供遠端協助	▪這個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」 ▪如果啟用這個原則設定，這部電腦上的使用者可使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助	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-33801-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用這個原則設定，這部電腦上的使用者無法使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助。 ▪如果未設定這個原則設定，這部電腦上的使用者無法使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助。 ▪如果啟用這個原則設定，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]。設定這個原則設定時，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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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> ▪如果啟用這個原則設定，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 ▪WindowsVista 和更新版本 啟用網域設定檔的遠端協助例			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					外。例外必須包含： Port135：TCP %WINDIR%\System32\msra.exe %WINDIR%\System32\raserver.exe WindowsXPServicePack2(SP2)和 WindowsXPProfessionalx64 版 ServicePack1(SP1) Port135：TCP %WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe %WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe %WINDIR%\System32\Sessmgr.exe 執行			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					WindowsServer2003ServicePack1(SP1)的電腦 Port135：TCP %WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe %WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe 允許遠端桌面例外			
40	Windows8.1 Computer Settings	TWGCB-01-004-0040	系統\遠端協助	設定請求遠端協助	▪這個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	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-35331-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					到這部電腦，使用者也可以設定其他遠端協助設定 ▪如果停用這個原則設定，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 ▪如果使用者未設定這個原則設定，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 ▪如果啟用這個原則設定，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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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)。這個原則設定在 WindowsVista 中無法使用，因為 SMAPI 是唯一支援的方法 ▪如果啟用這個原則設定，也應			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					該啟用適當的防火牆例外，以允許遠端協助通訊			
41	Windows8.1 Computer Settings	TWGCB-01-004-0041	系統\遠端協助	開啟工作階段紀錄	▪此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 ▪如果啟用這項原則設定，就會產生記錄檔 ▪如果停用此原則設定，就不會產生記錄檔 ▪如果沒有進行此設定，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	CCE-ID：CCE-33481-3
42	Windows8.1 Computer Settings	TWGCB-01-004-0042	系統\遠端程序呼叫	RPC 端點對應程式用戶端驗證	▪這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 ▪如果啟用這項原則設定，與端	電腦設定\系統管理範本\系統\遠端程序呼叫\RPC 端點對應	啟用	CCE-ID：CCE-35392-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用這項原則設定，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，才能套用這項原則	程式用戶端驗證		
43	Windows8.1 Computer Settings	TWGCB-01-004-0043	系統\遠端程序呼叫	未經驗證的RPC用戶端限制	▪ 這項原則設定決定未經驗證的 RPC 用戶端限制 ▪ 如果啟用此設定，它將會指示 RPC 伺服器上的 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	電腦設定\系統管理範本\系統\遠端程序呼叫\未經驗證的 RPC 用戶端限制	啟用：已驗證	CCE-ID：CCE-35391-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果啟用這項原則設定，則可使用下列值： (1)「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 (2)「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 (3)「已在無例外下驗證」：只允許已驗證的 RPC 用戶端(如			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
44	Windows8.1 Computer Settings	TWGCB-01-004-0044	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	▪這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 ▪如果啟用這項原則設定，在已安裝標準驅動程式時，不會傳送 Windows 錯誤報告 ▪如果停用或未設定這項原則設定，則在已安裝標準驅動程式時，會傳送 Windows 錯誤報告	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-35080-1
45	Windows8.1 Computer	TWGCB-01-0	系統\裝置安	在通常會提示	▪這項原則設定決定是否在通常會提示 Windows 建立系統還原	電腦設定\系統管理範本\系統\	停用	CCE-ID：CCE-34876-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0045	裝	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	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 ▪ 如果啟用這項原則設定，Windows 不會在通常會建立系統還原點的時候建立系統還原點 ▪ 如果停用或未設定這項原則設定，則 Windows 會依照正常方式建立系統還原點	裝置安裝\在通常會提示 Windows 建立系統還原點的裝置活動期間，防止 Windows 建立系統還原點		3
46	Windows8.1 Computer	TWGCB-01-0	系統\裝置安	指定搜尋裝置驅動	▪ 這項原則設定決定是否指定 Windows 搜尋裝置驅動程式的	電腦設定\系統管理範本\系統\	啟用 不搜尋	CCE-ID：CCE-33462-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0046	裝	程式的來源位置時的搜尋順序	來源位置時的搜尋順序 ▪如果啟用這項原則設定，使用者可以選擇讓 Windows 先搜尋 WindowsUpdate、後搜尋 WindowsUpdate，或不搜尋 WindowsUpdate ▪如果停用或未設定這項原則設定，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	裝置安裝\指定搜尋裝置驅動程式的來源位置時的搜尋順序	Windows Update	3
47	Windows8.1 Computer Settings	TWGCB-01-004-0047	系統\裝置安裝	允許遠端存取隨插即用介面	▪這項原則設定決定是否允許遠端存取隨插即用介面 ▪如果啟用這項原則設定，將允許從遠端連線到隨插即用介面 ▪如果停用或未設定這項原則設定，則不允許從遠端連線到隨	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-33972-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					插即用介面			
48	Windows8.1 Computer Settings	TWGCB-01-004-0048	系統\疑難排解與診斷	Microsoft 支援服務診斷工具：開啟與支援提供者的 MSDT 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 ▪ 如果保持這項原則設定為啟用狀態，使用者就能夠使用 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 ▪ 如果停用這項原則設定，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 ▪ 如果未設定這項原則設定，則預設啟用 MSDT 支援模式 ▪ 這項原則不需重新開機或重新	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：開啟與支援提供者的 MSDT 互動式通訊	停用	CCE-ID：CCE-34972-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					啟動服務就會生效：變更會立即生效			
49	Windows8.1 Computer Settings	TWGCB-01-004-0049	系統\疑難排解與診斷	啟用/停用 PrefTrack	▪這項原則設定決定要啟用或停用回應事件的追蹤 ▪如果啟用這項原則設定，就會處理並彙總回應事件。彙總的資料會透過 SQM 傳到 Microsoft ▪如果停用這項原則設定，就不會處理回應事件 ▪如果未設定這項原則設定，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-33662-8
50	Windows8.1 Computer Settings	TWGCB-01-004-005	系統\疑難排解與診	疑難排解：允許使用者從	▪這個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	電腦設定\系統管理範本\系統\疑難排解與診	停用	CCE-ID：CCE-35763-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		0	斷	「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)	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。 ▪ 如果啟用或未設定這個原則設定，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 ▪ 如果停用這個原則設定，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	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)		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					難排解服務的 Microsoft 伺服器			
51	Windows8.1 Computer Settings	TWGCB-01-004-0051	系統\Windows 時間服務\時間提供者	設定 Wndows NTP 用戶端	▪ 這項原則設定決定是否指定用於控制 WindowsNTP 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	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 ResolvePeerBackoff	CCE-ID： CCE-33661-0 CCE-34402-8 CCE-35135-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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，		MaxTimes：7 SpecialPollInterval：3600 EventLogFlags：0	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 3600 秒(1 小時) ▪ 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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
52	Windows8.1 Computer Settings	TWGCB-01-004-0052	系統	指定選用之元件安裝和元件修復的相關設定	▪ 這個原則設定會指定網路位置，用於修復損毀的作業系統以及啟用已經移除其裝載檔案的選用功能 ▪ 如果啟用這個原則設定並指定新的位置，修復損毀的作業系統以及啟用已經移除其裝載檔案的選用功能時，就會使用這個位置中的檔案。使用者必須在[其他來源檔案路徑]方塊中輸入新位置的完整路徑。使用者可以指定多個位置，但請使用分號隔開每一個路徑 ▪ 網路位置可以是資料夾或 WIM 檔案。如果它是一個 WIM 檔案，則位置最前面應該加上「wim：」並包含用於 WIM 檔	電腦設定\系統管理範本\系統\指定選用之元件安裝和元件修復的相關設定	啟用 不要從 Windows Update 下載裝載	CCE-ID：CCE-35079-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					案中的映像索引。例如"wim：\\server\share\install.wim：3" ▪ 如果停用或未設定這個原則設定，或者在這個原則設定所指定的位置中找不到必要的欄位，則如果電腦的原則設定允許，就會從 WindowsUpdate 下載檔案			
53	Windows8.1 Computer Settings	TWGCB-01-004-0053	網際網路通訊管理\網際網路通訊設定	關閉市集的存取權	▪ 這個原則設定指定是否使用市集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市集服務來尋找應用程式	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\關閉市集的存取權	啟用	CCE-ID：CCE-35626-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果啟用這個原則設定，將會移除[開啟檔案]對話方塊中的「在市集尋找應用程式」項目 ▪如果停用或未設定這個原則設定，使用者將可以使用市集服務，而且還可以在[開啟檔案]對話方塊中使用市集項目			
54	Windows8.1 Computer Settings	TWGCB-01-004-0054	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	▪這個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：這個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	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-35781-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					印。它只會禁止下載尚未在本機安裝的驅動程式 ▪ 如果啟用這個原則設定，將無法透過 HTTP 下載列印驅動程式 ▪ 如果停用或未設定這個原則設定，使用者可以透過 HTTP 下載列印驅動程式			
55	Windows8.1 Computer Settings	TWGCB-01-004-0055	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	▪ 這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快速連結。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	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-35425-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
56	Windows8.1 Computer Settings	TWGCB-01-004-005	網際網路通訊管理\	關閉網頁發布和線上訂購精	▪ 這項原則設定決定 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	電腦設定\系統管理範本\系統\網際網路通訊	啟用	CCE-ID：CCE-33143-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		6	網際網路通訊設定	靈的網際網路下載	▪ 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)	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		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
57	Windows8.1 Computer Settings	TWGCB-01-004-0057	網際網路通訊管理\網際網路通訊設定	關閉 HTTP 上的列印	▪這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：這個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-33783-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
58	Windows8.1 Computer Settings	TWGCB-01-004-0058	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	▪這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 ▪如果啟用這個原則設定，搜尋小幫手將不會在進行搜尋時下載內容更新 ▪如果停用或未設定這個原則設定，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	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-33817-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
59	Windows8.1 Computer Settings	TWGCB-01-004-0059	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	▪這項原則設定決定「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	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-33246-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					顯示這些工作			
60	Windows8.1 Computer Settings	TWGCB-01-004-0060	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	▪ 這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 TabletPC 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。這個工具會產生報告，然後透過安全的連線傳給 Microsoft ▪ 如果啟用這項原則，TabletPC 使用者無法選擇將手寫辨識個人化工具中的書寫範本與	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-32945-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Microsoft 共用 ▪ 如果停用這項原則，手寫辨識個人化工具中 TabletPC 使用者書寫範本將與 Microsoft 共用 ▪ 如果未做這個設定，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			
61	Windows8.1 Computer Settings	TWGCB-01-004-0061	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	▪ 這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。	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-35784-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 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 ▪ 如果啟用這項原則，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 ▪ 如果停用這項原則，則 TabletPC 使用者可以將手寫辨識錯誤報告給 Microsoft ▪ 如果未設定這項原則，則 TabletPC 使用者可以將手寫辨識錯誤報告給 Microsoft			
62	Windows8.1 Computer Settings	TWGCB-01-004-0062	網際網路通訊管理\網際網	關閉「訂購沖印」圖片工作	▪ 這項原則設定指定「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	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路	啟用	CCE-ID：CCE-34061-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			路通訊設定		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	通訊設定\關閉「訂購沖印」圖片工作		
63	Windows8.1 Computer Settings	TWGCB-01-004-0063	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	▪這個原則設定指定 Windows 註冊精靈是否可以連線到 Microsoft.com 進行線上註冊 ▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，則使用者可以連線到	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-33216-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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)			
64	Windows8.1 Computer Settings	TWGCB-01-004-0064	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	▪這個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 ▪如果啟用這個原則設定，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	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	啟用	CCE-ID：CCE-33153-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的 ISP 清單 ▪ 如果停用或未設定這個原則設定，使用者將可以連線到 Microsoft 下載其區域的 ISP 清單	路連線精靈		
65	Windows8.1 Computer Settings	TWGCB-01-004-0065	網際網路通訊管理\網際網路通訊設定	關閉 Windows 錯誤報告	▪ 這個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 ▪ 如果啟用這個原則設定，使用者將無法報告錯誤 ▪ 如果停用或未設定這個原則設定，可以透過網際網路或公司的檔案共用向 Microsoft 報告錯誤。 這個原則設定會覆寫任何從控	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-34260-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
66	Windows8.1 Computer Settings	TWGCB-01-004-0066	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	▪這個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	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-33204-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，使用者將可以使用網站服務			
67	Windows8.1 Computer Settings	TWGCB-01-004-0067	網際網路通訊管理\網際網路通訊設定	關閉 Windows Messenger 客戶經驗改善計畫	▪這個原則設定指定 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 ▪如果啟用這個原則設定，Windows Messenger 將不會收	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 客戶經驗改善計畫	啟用	CCE-ID：CCE-33957-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用這個原則設定，Windows Messenger 將收集匿名使用資訊，而且不會顯示該設定 ▪ 如果未設定這個原則設定，使用者將能選擇參加，並允許資料收集			
68	Windows8.1 Computer Settings	TWGCB-01-004-0068	進階稽核原則設定	稽核原則： 帳戶登入：稽核驗證認證	▪ 認證驗證 ▪ 這個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	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：	成功與失敗	CCE-ID：CCE-35494-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪數量：在網域控制站上是「高」 ▪用戶端版本的預設值：沒有稽核 ▪伺服器版本的預設值：成功	稽核驗證認證		
69	Windows8.1 Computer Settings	TWGCB-01-004-0069	進階稽核原則設定	稽核原則：帳戶管理：電腦帳戶管理	▪這個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 ▪如果設定這個原則，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 ▪如果未設定這個原則，則不會在電腦帳戶變更時產生稽核事	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：電腦帳戶管理	成功	CCE-ID：CCE-33410-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					件			
70	Windows8.1 Computer Settings	TWGCB-01-004-0070	進階稽核原則設定	稽核原則：帳戶管理：其他帳戶管理事件	▪ 這個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	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：其他帳戶管理事件	成功與失敗	CCE-ID：CCE-35497-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
71	Windows8.1 Computer Settings	TWGCB-01-004-0071	進階稽核原則設定	稽核原則：帳戶管理：安全性群組管理	▪這個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 ▪如果設定這個原則設定，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	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：安全性群組管理	成功與失敗	CCE-ID：CCE-35498-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					失敗嘗試 ▪如果未設定這個原則設定，則不會在安全性群組變更時產生稽核事件			
72	Windows8.1 Computer Settings	TWGCB-01-004-0072	進階稽核原則設定	稽核原則：帳戶管理：使用者帳戶管理	▪這個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 ▪如果設定這個原則設定，則會	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：使用者帳戶管理	成功與失敗	CCE-ID：CCE-35499-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪如果未設定這個原則設定，則不會在使用者帳戶變更時產生稽核事件			
73	Windows8.1 Computer Settings	TWGCB-01-004-0073	進階稽核原則設定	稽核原則：詳細追蹤：建立處理程序	▪這個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 ▪如果設定這個原則設定，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 ▪如果未設定這個原則設定，則	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\詳細追蹤\稽核原則：詳細追蹤：建立處理程序	成功	CCE-ID：CCE-33040-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					不會在建立處理程序時產生稽核事件			
74	Windows8.1 Computer Settings	TWGCB-01-004-0074	進階稽核原則設定	稽核原則：登入-登出：帳戶鎖定	▪此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\稽核原則\登入/登出\稽核原則：登入-登出：帳戶鎖定	成功與失敗	CCE-ID：CCE-35504-0
75	Windows8.1 Computer Settings	TWGCB-01-004-007	進階稽核原則設定	稽核原則：登入-登出：登	▪這個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	電腦設定\Windows 設定\安全性設定\進階稽核原則設	成功	CCE-ID：CCE-35507-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		5		出	在使用者帳戶登入的電腦上產生安全性稽核事件 ▪如果設定這個原則設定，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 ▪如果未設定這個原則設定，則不會在關閉登入工作階段時產生稽核事件	定\系統稽核原則\登入/登出\稽核原則：登入-登出：登出		
76	Windows8.1 Computer Settings	TWGCB-01-004-0076	進階稽核原則設定	稽核原則：登入-登出：登入	▪這個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	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\	成功與失敗	CCE-ID：CCE-35508-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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」。	稽核原則：登入-登出：登入		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					網域控制站或網路伺服器上是「中」 ▪用戶端版本的預設值：成功 ▪伺服器版本的預設值：成功，失敗			
77	Windows8.1 Computer Settings	TWGCB-01-004-0077	進階稽核原則設定	稽核原則：登入-登出：特殊登入	▪這個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	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：特殊登入	成功	CCE-ID：CCE-35511-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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) ▪ 數量：低 ▪ 預設值：成功			
78	Windows8.1 Computer Settings	TWGCB-01-004-0078	進階稽核原則設定	稽核原則：物件存取：卸除式存放裝置	▪ 此原則設定可稽核存取卸除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，每當有帳戶存取卸除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	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：卸除式存放裝置	成功	CCE-ID：CCE-35520-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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，當有帳戶存取卸除式存放裝置上的檔案系統物件時，就不會產生稽核事件			
79	Windows8.1 Computer Settings	TWGCB-01-004-0079	進階稽核原則設定	稽核原則：原則變更：稽核原則變更	▪這個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	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：稽核原則變更	成功與失敗	CCE-ID：CCE-35521-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-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 ▪ 如果設定這個原則設定，則會在嘗試遠端 RPC 連線時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這個原則設定，則不會在嘗試遠端 RPC 連線時產生稽核事件			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
80	Windows8.1 Computer Settings	TWGCB-01-004-0080	進階稽核原則設定	稽核原則：原則變更：驗證原則變更	▪這個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	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：驗證原則變更	成功	CCE-ID：CCE-33091-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的名稱與現有命名空間名稱相同時 ▪如果設定這個原則設定，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 ▪如果未設定這個原則設定，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			
81	Windows8.1 Computer Settings	TWGCB-01-004-0081	進階稽核原則設定	稽核原則：特殊權限使用：機密	▪這個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	電腦設定\Windows 設定\安全性設定\進階稽核原則	成功與失敗	CCE-ID：CCE-35524-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				特殊權限使用	-呼叫下列其中一種權限： 當成作業系統的一部分 -備份檔案及目錄 -建立權杖物件 -偵錯程式 -讓電腦及使用者帳戶受信賴，以進行委派 -產生安全性稽核 -在驗證後模擬用戶端 -載入及解除載入裝置驅動程式 -管理稽核及安全性記錄檔 -修改韌體環境值 -取代處理程序等級權杖 -還原檔案及目錄 -取得檔案或其他物件的擁有權 ▪如果設定這個原則設定，則會	設定\系統稽核原則\特殊權限使用\稽核原則：特殊權限使用：機密特殊權限使用		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 如果未設定這個原則設定，則不會進行機密特殊權限要求時產生稽核事件			
82	Windows8.1 Computer Settings	TWGCB-01-004-0082	進階稽核原則設定	稽核原則：系統：IPSEC 驅動程式	▪ 這個原則設定可稽核因 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	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：IPSEC 驅動程式	成功與失敗	CCE-ID：CCE-35525-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-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 ▪如果設定這個原則設定，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 ▪如果未設定這個原則設定，則不會在 IPsec 篩選器驅動程式操作上產生稽核事件			
83	Windows8.1 Computer Settings	TWGCB-01-004-0083	進階稽核原則設定	稽核原則：系統：其他系統事件	▪這個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	電腦設定\Windows 設定\安全性設定\進階稽核原則設	失敗	CCE-ID：CCE-32936-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-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	定\稽核原則\系統\稽核原則：系統：其他系統事件		
84	Windows8.1 Computer Settings	TWGCB-01-004-0084	進階稽核原則設定	稽核原則：系統：安全性狀態變更	▪這個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：安全性狀態變更	成功與失敗	CCE-ID：CCE-33043-1
85	Windows8.1 Computer Settings	TWGCB-01-004-008	進階稽核原則設定	稽核原則：系統：安全	▪這個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：	電腦設定\Windows 設定\安全性設定\	成功與失敗	CCE-ID：CCE-35526-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		5		性系統延伸	-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 ▪如果設定這個原則設定，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 ▪如果未設定這個原則設定，則	進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：安全性系統延伸		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					不會在嘗試載入安全性系統延伸時產生稽核事件			
86	Windows8.1 Computer Settings	TWGCB-01-004-0086	進階稽核原則設定	稽核原則：系統：系統完整性	▪這個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	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：系統完整性	成功與失敗	CCE-ID：CCE-35527-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					操作			
87	Windows8.1 Computer Settings	TWGCB-01-004-0087	安全性選項\帳戶	帳戶：Administrator 帳戶狀態	▪ 這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-33511-7
88	Windows8.1 Computer Settings	TWGCB-01-004-0088	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	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	使用者無法新增 Microsoft 帳戶或以 Microsoft 帳戶登入	CCE-ID：CCE-35487-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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	帳戶		
89	Windows8.1 Computer	TWGCB-01-0	安全性選項\	帳戶：Guest 帳	▪ 這項原則設定決定啟用或停用 Guest 帳戶	電腦設定\Windows 設定\	停用	CCE-ID：CCE-33949-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0089	帳戶	戶狀態	▪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	安全性設定\本機原則\安全性選項\帳戶：Guest 帳戶狀態		9
90	Windows8.1 Computer Settings	TWGCB-01-04-0090	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	▪這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： (1)不是位於實際安全位置的電腦，應一直針對所有本機使用	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-32929-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (2)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 (3)這個設定對於使用網域帳戶的登入沒有影響 (4)應用程式若使用遠端互動式登入，則可以跳過這個設定 (5)遠端桌面服務在舊版的 Windows 作業系統中稱為「終端機服務」			
91	Windows8.1 Computer	TWGCB-01-0	安全性選項\	帳戶：重新命名系	▪ 這項原則設定將重新命名已知的 Administrator 帳戶，透過使	電腦設定\Windows 設定\	Renamed_Admin	CCE-ID：CCE-33034-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0091	帳戶	統管理員帳戶	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	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		0
92	Windows8.1 Computer Settings	TWGCB-01-004-0092	安全性選項\帳戶	帳戶：重新命名來賓帳戶名稱	▪ 這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-35488-6
93	Windows8.1 Computer Settings	TWGCB-01-004-0093	安全性選項\帳戶	稽核：稽核通用系統物件的存取	▪ 這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、	電腦設定\Windows 設定\安全性設定\本機原則\安全性	停用	CCE-ID：CCE-33093-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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：設定這項原則設定時，在重新啟動 Windows 之後，所做的變更才會生效	選項\稽核：稽核通用系統物件的存取		
94	Windows8.1 Computer Settings	TWGCB-01-004-0094	安全性選項\稽核	稽核：稽核備份與還原權限的使用	▪ 這項原則設定決定在「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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：稽	停用	CCE-ID：CCE-33045-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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： (1)在 WindowsVista 之前的 Windows 版本中設定這項原則設定，所做的變更在重新啟動 Windows 之後才會生效 (2)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	核備份與還原權限的使用		
95	Windows8.1 Computer Settings	TWGCB-01-004-0095	安全性選項\稽核	稽核：強制執行稽核原則子類別設定	▪ WindowsVista 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	電腦設定\Windows 設定\安全性設定\本機原則\安全性	啟用	CCE-ID：CCE-35533-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				(WindowsVista 或更新版本)以覆寫稽核原則類別設定	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 WindowsVista 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 WindowsVista 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	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		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					錄機碼			
96	Windows8.1 Computer Settings	TWGCB-01-004-0096	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	▪這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 ▪如果啟用了這項安全性設定，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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\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-33046-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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。直到這項安全性設定重設之前，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 ▪注意：在 WindowsVista 之前的 Windows 版本設定此安全性設定時，變更要等到重新啟動 Windows 之後才會生效			
97	Windows8.1 Computer Settings	TWGCB-01-004-0097	安全性選項\裝置	裝置：允許格式化以及退出卸除式媒	▪此安全性設定決定允許哪些人格式化和退出卸除式 NTFS 媒體 ▪此功能可指定給：	電腦設定\Windows 設定\安全性設定\本機原則\安全	Administrators and Interactive Users	CCE-ID：CCE-34355-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				體	-Administrators -Administrators 以 InteractiveUsers	性選項\裝置：允許格式化以及退出卸除式媒體		
98	Windows8.1 Computer Settings	TWGCB-01-004-0098	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	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-33958-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					時，都可以安裝印表機驅動程式 ▪伺服器預設值：已啟用 ▪工作站預設值：已停用 ▪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。			
99	Windows8.1 Computer Settings	TWGCB-01-004-0099	安全性選項\裝置	裝置：CD-ROM 存取只限於登入本機的使用者	▪此安全性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卸除式 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	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-33512-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					CD-ROM ▪ 預設值：未定義此原則，且 CD-ROM 取並未僅限於本機登入的使用者			
100	Windows8.1 Computer Settings	TWGCB-01-004-0100	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	▪ 此安全性設定決定本機使用者和遠端使用者是否能同時存取卸除式軟碟機媒體 ▪ 如果啟用此原則，便只允許以互動方式登入的使用者存取卸除式軟碟機媒體。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-35294-8
101	Windows8.1	TWGC	安全性	網域成	▪ 這項原則設定決定，網域成員	電腦設定	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0101	選項\網域成員	員：安全通道資料加以數位加密或簽章(自動)	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 LSASID/名稱查詢的操作 ▪ 這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 ▪ 如果啟用這項原則，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	\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)		CCE-34892-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					如果停用這項原則，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： (1)網域成員：安全通道資料加以數位加密(可能的話) (2)網域成員：安全通道資料加以數位簽章(自動) ▪注意： (1)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 (2)透過安全通道傳輸的登入資			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
102	Windows8.1 Computer Settings	TWGCB-01-004-0102	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)	▪ 這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 LSASID/名稱查詢之類的操作 ▪ 如果啟用這項原則設定，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，	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-35273-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用這項原則設定，則網域成員不會嘗試交涉安全通道加密			
103	Windows8.1 Computer Settings	TWGCB-01-004-0103	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)	▪ 這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 LSASID/名稱查詢的操作	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-34893-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果啟用這項原則設定，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篡改 ▪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)」，則會假設這項原則為啟用狀態，無論目前設定為何			
104	Windows8.1 Computer Settings	TWGCB-01-0004-0104	安全性選項\網域成員	網域成員：停用電腦帳戶密碼變更	▪這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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成	停用	CCE-ID：CCE-34986-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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： (1)這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 (2)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	員:停用電腦帳戶密碼變更		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					兩個安裝			
105	Windows8.1 Computer Settings	TWGCB-01-004-0105	安全性選項\網域成員	網域成員：最長電腦帳戶密碼有效期	▪ 這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	CCE-ID：CCE-34894-6
106	Windows8.1 Computer Settings	TWGCB-01-004-0106	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	▪ 這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	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-35177-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					LSASID/名稱查詢之類的操作 ▪如果啟用這項原則設定，除非能執行 128 位元加密，否則不會建立安全通道 ▪如果停用這項原則設定，則會與網域控制站交涉金鑰長度			
107	Windows8.1 Computer Settings	TWGCB-01-0004-0107	安全性選項\互動式登入	互動式登入：不要顯示上次登入的使用者名稱	▪這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：不要顯示上次登入的使用者名稱	啟用	CCE-ID：CCE-34898-7
108	Windows8.1 Computer	TWGCB-01-0	安全性選項\	互動式登入：不要	▪這項原則設定決定是否需要按 CTRL+ALT+DEL 後，使用者才	電腦設定\Windows 設定\	停用	CCE-ID：CCE-35099-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0108	互動式登入	求按 CTRL+ALT+DEL 鍵	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)	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		1
109	Windows8.1 Computer Settings	TWGCB-01-004-010	安全性選項\互動式	互動式登入：電腦帳戶閾值	▪ 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	電腦設定\Windows 設定\安全性設定\本	5 次不正確的登入嘗試	CCE-ID：CCE-34899-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		9	登入		適當的修復密碼備份原則 ▪此安全性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 ▪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	機原則\安全性選項\互動式登入：電腦帳戶閾值		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					適當的修復密碼備份原則			
110	Windows8.1 Computer Settings	TWGCB-01-004-0110	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	CCE-ID：CCE-34900-1
111	Windows8.1 Computer Settings	TWGCB-01-004-0111	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 ▪若網域控制站無法使用，且已快取使用者的登入資訊時，則會以下列訊息提示使用者：「Windows 無法連線至伺服器以確認使用者的登入設定。已	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	CCE-ID：CCE-34901-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					使用先前儲存的帳戶資訊讓使用者登入。如果使用者上次登入這台電腦後，曾經變更過使用者的帳號資訊，使用者所做的變更不會反應在這個工作階段中」 ▪ 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：「系統目前無法讓使用者登入，因為網域<DOMAIN_NAME>無法使用」 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			
112	Windows8.1 Computer	TWGCB-01-0	安全性選項\	互動式登入：在密	▪ 這項原則設定決定在使用者的密碼即將到期時，要提前多久	電腦設定\Windows 設定\	14 天	CCE-ID：CCE-35274-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0112	互動式登入	碼到期前提示使用者變更密碼	(天數)事先提醒使用者	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		0
113	Windows8.1 Computer Settings	TWGCB-01-004-0113	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-34902-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
114	Windows8.1 Computer Settings	TWGCB-01-004-0114	安全性選項\互動式登入	互動式登入：智慧卡移除操作	▪這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： (1)無動作 (2)鎖定工作站 (3)強制登出 (4)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」，	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-34988-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 注意：遠端桌面服務在舊版的 Windows Server 中稱為「終端機服務」 ▪ 預設值：未定義此原則，這表示系統會將它視為 [無動作] ▪ 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			
115	Windows8.1	TWGC	安全性	Microsoft	▪ 此安全性設定決定 SMB 用戶	電腦設定	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0115	選項\Microsoft 網路用戶端	網路用戶端：數位簽章用戶端的通訊(自動)	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	\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)		CCE-35222-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					器之間交涉 SMB 封包簽章 ▪ 預設值：已停用 ▪ 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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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： (1) 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 (2) 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 (3) Microsoft 網路伺服器：數位簽章伺服器的通訊 (自動) - 控			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					制伺服器端 SMB 元件是否需要封包簽章 (4) 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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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%			
116	Windows8.1 Computer Settings	TWGCB-01-004-0116	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)	▪ 這項原則設定決定 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	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-34908-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 這項原則設定決定 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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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： (1)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 (2)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 (3)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(4)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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%			
117	Windows8.1 Computer Settings	TWGCB-01-004-0117	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	▪如果啟用這項原則設定，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 MB 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-33717-0
118	Windows8.1 Computer	TWGCB-01-0	安全性選項	Microsoft 網路伺服	▪這項原則設定決定伺服器訊息區(SMB)工作階段的連續閒置	電腦設定\Windows 設定\	15 分鐘	CCE-ID：CCE-34909-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0118	\Microsoft 網路伺服器	器：暫停工作階段前，要求的閒置時間	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	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		2
119	Windows8.1 Computer Settings	TWGCB-01-004-0119	安全性選項\Microsoft 網路	Microsoft 網路伺服器：數位簽章伺服	▪ 這項原則設定決定 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	電腦設定\Windows 設定\安全性設定\本機原則\安全性	啟用	CCE-ID：CCE-35065-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			伺服器	器的通訊(自動)	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。這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	選項\Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 Windows2000 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： (1)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 (2)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					是否啟用封包簽章 (3)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 (4)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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%			
120	Windows8.1 Computer Settings	TWGCB-01-0004-0120	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	▪ 這項原則設定決定 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	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	啟用	CCE-ID：CCE-35182-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				戶端同意)	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。這項原則設定決定 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	位簽章伺服器的通訊(如果用戶端同意)		
121	Windows8.1 Computer Settings	TWGCB-01-004-012	安全性選項\Micros	Microsoft 網路伺服器：當登	▪ 這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	電腦設定\Windows 設定\安全性設定\本	啟用	CCE-ID：CCE-34911-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		1	oft 網路伺服器	入時數到期時，中斷用戶端連線	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，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	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		
122	Windows8.1 Computer Settings	TWGCB-01-004-0122	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	▪這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： (1)關閉：SMB 伺服器不需要或不會驗證 SMB 用戶端的 SPN (2)如果是用戶端所提供則接受：SMB 伺服器將會接受與驗	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-35299-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (3)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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。這個設定會影響伺服器 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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
123	Windows8.1 Computer Settings	TWGCB-01-004-0123	安全性選項\MSS	MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended)	▪ 這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	CCE-ID：CCE-35438-1
124	Windows8.1 Computer Settings	TWGCB-01-004-0124	安全性選項\MSS	MSS：(DisableIPSourceRouting IPv6) IP	▪ IPsourcerouting 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 ▪ 這項原則設定決定 IP source routing 防護層級(決定作業系	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：	Highest protection，source routing is completely	CCE-ID：CCE-33790-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				source routing protection level (protects against packet spoofing)	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： (1)設為 No additional protection：代表作業系統接受與轉送來源路由封包 (2)設為 Medium，代表作業系統接受但不轉送來源路由封包 (3)設為 Highestprotection，代表作業系統完全拒絕來源路由封包	(DisableIPSourceRouting IPv6)IP source routing protection level(protects against packet spoofing)	disabled	
125	Windows8.1 Computer Settings	TWGCB-01-004-0125	安全性選項\MSS	MSS：(DisableIPSourceRouting) IP source routing	▪ 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 ▪ 這項原則設定決定 IP source	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(DisableIPSour	Highest protection，source routing is completely disabled	CCE-ID：CCE-33816-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				protection level (protects against packet spoofing)	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： (1)設為 No additional protection：代表作業系統接受與轉送來源路由封包 (2)設為 Medium，代表作業系統接受但不轉送來源路由封包 (3)設為 Highestprotection，代表作業系統完全拒絕來源路由封包	ceRouting)IP source routing protection level(protects against packet spoofing)		
126	Windows8.1 Computer Settings	TWGCB-01-004-0126	安全性選項\MSS	▪ MSS：(EnableICMPRedirect)Allow ICMP	▪ 這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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：	停用	CCE-ID：CCE-34597-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				redirects to override OSPF generated routes	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	(EnableICMPRedirect)Allow ICMP redirects to override OSPF generated routes		
127	Windows8.1 Computer Settings	TWGCB-01-004-0127	安全性選項\MSS	MSS：(Hidden) Hide Computer From the Browse List (not recomme	▪這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	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	啟用	CCE-ID：CCE-33814-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				nded except for highly secure environments)	訊	List(not recommended except for highly secure environments)		
128	Windows8.1 Computer Settings	TWGCB-01-004-0128	安全性選項\MSS	MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds	▪ 這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 ▪ 這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	300000or5 minutes (recommended)	CCE-ID：CCE-35469-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
129	Windows8.1 Computer Settings	TWGCB-01-004-0129	安全性選項\MSS	MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.	▪這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： (1)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」 (2)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」 (3)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」 (4)設定為 3：代表「只有 ISAKMP 流量是免除 IPSec 篩	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)	CCE-ID：CCE-33792-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					選功能」			
130	Windows8.1 Computer Settings	TWGCB-01-004-0130	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 ▪ 這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	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	CCE-ID：CCE-35405-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
131	Windows8.1 Computer Settings	TWGCB-01-004-0131	安全性選項\MSS	MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default	▪ 這項原則設定決定是否允許 InternetRouterDiscoveryProtocol(IRDP)自動偵測與設定預設 Gateway 位址 ▪ 設定選項如下： (1)停用 (2)啟用 (3)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	停用	CCE-ID：CCE-34614-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				Gateway addresses (could lead to DoS)		configure Default Gateway addresses(could lead to DoS)		
132	Windows8.1 Computer Settings	TWGCB-01-004-0132	安全性選項\MSS	MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended)	▪ 這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： (1)應用程式被載入的目錄 (2)系統目錄 (3)16 位元系統目錄(如果有的話) (4)Windows 目錄 (5)目前目錄 (6)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	CCE-ID：CCE-34022-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果設定為停用：搜尋 DLL 的順序如下， (1)應用程式被載入的目錄 (2)目前目錄 (3)系統目錄 (4)16 位元系統目錄(如果有的話) (5)Windows 目錄 (6)在 PATH 環境變數中列出來的目錄			
133	Windows8.1 Computer Settings	TWGCB-01-004-0133	安全性選項\MSS	MSS：(ScreenSaverGracePeriod) The time in seconds	▪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。這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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(ScreenSaverGracePeriod)The	5	CCE-ID：CCE-34619-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				before the screen saver grace period expires (0 recommended)	的任何數值	time in seconds before the screen saver grace period expires(0 recommended)		
134	Windows8.1 Computer Settings	TWGCB-01-004-0134	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknow	▪ 這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	3	CCE-ID：CCE-34622-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				ledged data is retransmitted (3 recommended, 5 is default)		unacknowledged data is retransmitted(3 recommended，5 is default)		
135	Windows8.1 Computer Settings	TWGCB-01-004-0135	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is	▪ 這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 unacknowledge	3	CCE-ID：CCE-34623-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				retransmitted (3 recommended, 5 is default)		d data is retransmitted(3 recommended，5 is default)		
136	Windows8.1 Computer Settings	TWGCB-01-004-0136	安全性選項\MSS	MSS：(Warning Level) Percentage threshold for the security event log at which the system	▪ 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	90	CCE-ID：CCE-35406-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				will generate a warning		generate a warning		
137	Windows8.1 Computer Settings	TWGCB-01-004-0137	安全性選項\網路存取	網路存取：允許匿名 SID/名稱轉譯	▪這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-34914-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
138	Windows8.1 Computer Settings	TWGCB-01-004-0138	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	▪ 這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-34723-7
139	Windows8.1 Computer Settings	TWGCB-01-004-0139	安全性選項\網路存取	網路存取：不允許 SAM 帳戶的匿名列舉	▪ 這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	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	啟用	CCE-ID：CCE-34631-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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	SAM 帳戶的匿名列舉		
140	Windows8.1 Computer Settings	TWGCB-01-004-0140	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	▪ 這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：設定這項原則設定時，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-33718-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
141	Windows8.1 Computer Settings	TWGCB-01-004-0141	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	▪這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	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-35367-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
142	Windows8.1 Computer Settings	TWGCB-01-004-0142	安全性選項\網路存取	網路存取：可以匿名存取的具名管道	▪ 這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-34965-4
143	Windows8.1 Computer Settings	TWGCB-01-004-0143	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	▪ 此安全性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	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	▪ Software\Microsoft\Windows NT\CurrentVersion\P	CCE-ID：CCE-35300-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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。 ▪ 注意：在 Windows XP 中，此安全性設定稱為「網路存取：可遠端存取的登錄路徑」。如果使用者在加入網域的 Windows Server 2003 系列成員中設定此設定，則執行 Windows XP 的電腦會繼承此設定，但將以「網路存取：可遠端存取的登錄路徑」安全性選項顯示。如需詳細資訊，請參閱「網路存取：可遠端存取的登錄路徑及子路徑。」	的登錄路徑及子路徑	rint ▪ Software\Microsoft\Windows NT\CurrentVersion\Windows ▪ System\CurrentControlSet\Control\Print\Printers ▪ System\CurrentControlSet\Servi	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							ces\Eventlog ▪ Software\Microsoft\OLAP Server ▪ System\CurrentControlSet\Control\ContentIndex ▪ System\CurrentControlSet\Control\Termin	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							al Server ▪ System\CurrentControlSet\Control\Terminal Server\UserConfig ▪ System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguratio	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							n ▪ Software\Microsoft\Windows NT\CurrentVersion\Perflib ▪ System\CurrentControlSet\Services\SysmonLog	
144	Windows8.1 Computer Settings	TWGCB-01-004-014	安全性選項\網路存	網路存取：可遠端存取的	▪ 這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	電腦設定\Windows 設定\安全性設定\本	▪ System\CurrentContr	CCE-ID：CCE-33976-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		4	取	登錄路徑	(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	機原則\安全性選項\網路存取:可遠端存取的登錄路徑	olSet\Control\ProductOptions ▪ System\CurrentControlSet\Control\Server Applications ▪ Software\Microsoft\Windows NT\CurrentVersion	
145	Windows8.1	TWGC	安全性	網路存	▪啟用這項原則設定時，會將共	電腦設定	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0145	選項\網路存取	取：限制匿名存取具名管道和共用	用和管道的匿名存取限制為以下設定： (1)網路存取：可以匿名存取的具名管道 (2)網路存取：可以匿名存取的共用	\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		CCE-33563-8
146	Windows8.1 Computer Settings	TWGCB-01-004-0146	安全性選項\網路存取	網路存取：可以匿名存取的共用	▪ 這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-34651-0
147	Windows8.1 Computer Settings	TWGCB-01-004-014	安全性選項\網路存	網路存取：共用和安全性	▪ 這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」，則使	電腦設定\Windows 設定\安全性設定\本	傳統-本機使用者以自身身分	CCE-ID：CCE-33719-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		7	取	模式用於本機帳戶	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」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」，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」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： (1)使用「僅適用於來賓」模式，	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	驗證	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (2)使用「傳統」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			
148	Windows8.1 Computer Settings	TWGCB-01-004-0148	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	▪ 這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 ▪ 如果啟用這項原則設定，以 Local System 執行且使用交涉的服務會使用電腦身分識別。	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	啟用	CCE-ID：CCE-33141-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果未設定這項原則設定，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 Windows7 或 Windows Server 2008 R2 才支援此原則	NTLM 使用電腦身分識別		
149	Windows8.1 Computer Settings	TWGCB-01-004-0149	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	停用	CCE-ID：CCE-35410-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						LocalSystem NULL 工作階段回復		
150	Windows8.1 Computer Settings	TWGCB-01-004-0150	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	CCE-ID：CCE-35411-8
151	Windows8.1 Computer Settings	TWGCB-01-004-0151	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	▪這項原則將設定允許 Kerberos 使用的加密類型 ▪如果未選取，則不允許加密類型。這個設定可能會影響與用戶端電腦或服務及應用程式的	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	RC4_HMAC_MD5 AES128_HMAC_SHA1	CCE-ID：CCE-35786-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					相容性 ▪ 這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	性：設定 Kerberos 允許的加密類型	AES256_HMAC_SHA1 未來的加密類型	
152	Windows8.1 Computer Settings	TWGCB-01-004-0152	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	▪ 這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： (1)Windows 2000 Service Pack	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-35225-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (2)此設定會影響執行 Windows 2000 Server、Windows 2000 Professional、Windows XP 及 Windows Server 2003 系列的電腦與執行 Windows 95 和 Windows 98 的電腦進行通訊的能力			
153	Windows8.1 Computer Settings	TWGCB-01-004-0153	安全性選項\網路安全性	網路安全性：強制限制登入時數	▪ 這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	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-34993-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
154	Windows8.1 Computer Settings	TWGCB-01-004-0154	安全性選項\網路安全性	網路安全性：LAN Manager 驗證等級	▪這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： (1)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	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-35302-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(2)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 (3)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 (4)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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					NTLMv2 驗證 (5)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) (6)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) 注意：此設定會影響執行 Windows 2000 Server、Windows 2000 Professional、Windows XP Professional 及 Windows Server			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					2003 系列之電腦與執行 Windows NT 4.0 或更舊版本的電腦進行網路通訊的能力。例如，目前執行 Windows NT 4.0 SP4 或更舊版本的電腦並不支援 NTLMv2。執行 Windows 95 和 Windows 98 的電腦不支援 NTLM			
155	Windows8.1 Computer Settings	TWGCB-01-004-0155	安全性選項\網路安全性	網路安全性：LDAP 用戶端簽章要求	▪這項原則設定決定代表發出 LDAPBIND 要求之用戶端所要求的資料簽章層級，選項如下： (1)無：LDAPBIND 要求隨呼叫者指定的選項發出 (2)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	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-33802-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					項初始化 LDAPBIND 要求。若已啟動 TLS\SSL，會隨呼叫者指定的選項初始化 LDAPBIND 要求 (3)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 LDAPBIND 命令要求失敗			
156	Windows8.1 Computer Settings	TWGCB-01-004-0156	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	▪ 這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 LANManager 驗證等級安全性設定值，選項如下： (1)要求 NTLMv2 工作階段安全性：若未交涉 NTLMv2 通訊協	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	要求 NTLMv2 工作階段安全性要求 128 位元加密	CCE-ID：CCE-35447-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				戶端的最小工作階段安全性	定，連線將會失敗 (2)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	全 RPC)用戶端的最小工作階段安全性		
157	Windows8.1 Computer Settings	TWGCB-01-004-0157	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	▪這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 LANManager 驗證等級安全性設定值，選項如下： (1)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 (2)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-35108-0
158	Windows8.1 Computer	TWGCB-01-0	安全性選項\	修復主控台：允許	▪這項原則設定決定是否必須在授與系統存取權之前提供	電腦設定\Windows 設定\	停用	CCE-ID：CCE-35228-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0158	修復主控台	自動系統管理登入	Administrator 帳戶的密碼 ▪如果啟用此選項，修復主控台不需要提供密碼，且將會自動登入系統	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		6
159	Windows8.1 Computer Settings	TWGCB-01-004-0159	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： (1)Allow Wild Cards：對某些命令啟用萬用字元支援(例如 DEL 命令) (2)Allow All Paths：允許存取電腦上的所有檔案和資料夾 (3)Allow Removable Media：允許將檔案複製到卸除式媒體，例如磁片	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-34757-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(4)No Copy Prompt：不要提示正在覆寫現有的檔案			
160	Windows8.1 Computer Settings	TWGCB-01-004-0160	安全性選項\關機	關機：允許不登入就將系統關機	▪這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-34628-8
161	Windows8.1 Computer Settings	TWGCB-01-004-0161	安全性選項\關機	關機：清除虛擬記憶體分頁檔	▪此安全性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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\關機：清	停用	CCE-ID：CCE-35005-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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。若啟用此安全性選項，當停用休眠時，也會清除休眠檔案(hiberfil.sys)	除虛擬記憶體分頁檔		
162	Windows8.1 Computer Settings	TWGCB-01-004-016	安全性選項\系統加	系統加密編譯：使用 FIPS	▪ 對於 Schannel Security Service Provider(SSP)，這項原則設定會停用強度較低的安全通訊端層	電腦設定\Windows 設定\安全性設定\本	啟用	CCE-ID：CCE-35641-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		2	密編譯	140 相容加密演算法，包括加密、雜湊以及簽署演算法	(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 核准的加密編譯演算法：3 DES 與 AES 用於加密、RSA 或 ECC 公開金鑰加密編譯用於 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	機原則\安全性選項\系統加密編譯：使用 FIPS 140 相容加密演算法，包括加密、雜湊以及簽署演算法		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(AES)加密演算法來加密 NTFS 檔案系統支援的檔案資料			
163	Windows8.1 Computer Settings	TWGCB-01-004-0163	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	▪ 這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	CCE-ID：CCE-35008-2
164	Windows8.1 Computer Settings	TWGCB-01-004-0164	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	▪ 此安全性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、	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\系統物	啟用	CCE-ID：CCE-35232-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				(例如：符號連結)	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	件：加強內部系統物件的預設權限 (例如：符號連結)		
165	Windows8.1 Computer Settings	TWGCB-01-004-0165	安全性選項\使用者帳戶控制	使用者帳戶控制：使用內建的 Administrator 帳戶	▪ 這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： (1)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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：使用內	啟用	CCE-ID：CCE-35338-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				的管理員核准模式	操作都會提示使用者核准操作 (2)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	建的 Administrator 帳戶的管理員核准模式		
166	Windows8.1 Computer Settings	TWGCB-01-004-0166	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升權限	▪ 這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	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升權限	停用	CCE-ID：CCE-35458-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
167	Windows8.1 Computer Settings	TWGCB-01-004-0167	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	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-33784-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
168	Windows8.1 Computer Settings	TWGCB-01-004-0168	安全性選項\使用者帳戶控制	使用者帳戶控制：標準使用者之提升權限提示的行為	▪ 這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： (1)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	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	在安全桌面顯示輸入認證	CCE-ID：CCE-33785-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					使用者輸入有效的認證，該操作會以適用的權限繼續執行 (2)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企業可能會選擇此設定，以降低需要尋求支援部門協助的機會 (3)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	用者之提升權限提示的行為		
169	Windows8.1 Computer	TWGCB-01-0	安全性選項\	使用者帳戶控制：	▪此原則設定會控制電腦的應用程式安裝偵測行為，選項如下:	電腦設定\Windows 設定\	啟用	CCE-ID：CCE-35429-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0169	使用者帳戶控制	偵測應用程式安裝，並提示提升權限	▪ 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)) 的企業，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	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		0
170	Windows8.1 Computer	TWGCB-01-0	安全性選項\	使用者帳戶控制：	▪ 這項原則設定將強制公開金鑰基礎結構(PKI)簽章檢查任何要	電腦設定\Windows 設定\	停用	CCE-ID：CCE-33786-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0170	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	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： (1)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 (2)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	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		5
171	Windows8.1 Computer Settings	TWGCB-01-004-0171	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	▪ 這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： (1)…\ProgramFiles\，包含子目	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	啟用	CCE-ID：CCE-35401-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				應用程式，提高其權限	錄 (2)…\Windows\system32\ (3)…\ProgramFiles(x86)\，包含64位元Windows版本的子目錄 注意：不論這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： (1)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 (2)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	在安全位置安裝的 UIAccess 應用程式，提高其權限		
172	Windows8.1	TWGC	安全性	使用者帳	▪此原則設定會控制電腦的所有	電腦設定	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0172	選項\使用者帳戶控制	戶控制：所有系統管理員均以管理員核准模式執行	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	\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		CCE-33788-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
173	Windows8.1 Computer Settings	TWGCB-01-004-0173	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	▪這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： (1)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 (2)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-33815-2
174	Windows8.1 Computer Settings	TWGCB-01-004-0174	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	▪這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 ▪此原則設定可減少那些以系統管理員身分執行，並將執行階	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	啟用	CCE-ID：CCE-35459-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				化並儲存至每一使用者位置	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： (1)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 (2)停用：將資料寫入至受保護位置的應用程式失敗	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		
175	Windows8.1 Computer Settings	TWGCB-01-004-0175	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 ▪注意：遠端桌面服務在舊版的	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	Administrators	CCE-ID：CCE-32928-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					WindowsServer 中稱為「終端機服務」	腦		
176	Windows8.1 Computer Settings	TWGCB-01-004-0176	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 ▪如果機關僅使用 Windows Server 2003 系列成員的伺服器，則無需將此特殊權限指派給使用者。不過，如果機關使用執行 Windows 2000 或 Windows NT 4.0 的伺服器，則	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-35403-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					可能需要指派此特殊權限，以使用以純文字交換密碼的應用程式 ▪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			
177	Windows8.1 Computer Settings	TWGCB-01-004-0177	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-35490-2
178	Windows8.1 Computer Settings	TWGCB-01-004-0178	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	電腦設定\Windows 設定\安全性設定\本機原則\使用者	Administrators，Users	CCE-ID：CCE-35640-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					容性	權限指派\允許本機登入		
179	Windows8.1 Computer Settings	TWGCB-01-004-0179	使用者權限指派	允許透過遠端桌面服務登入	▪這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 ▪注意：此設定對於尚未升級至 Service Pack2 的 Windows 2000 電腦沒有任何影響	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\允許透過遠端桌面服務登入	Remote Desktop Users，Administrators	CCE-ID：CCE-33035-7
180	Windows8.1 Computer Settings	TWGCB-01-004-0180	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：	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-35699-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-Backup Operators -Server Operators			
181	Windows8.1 Computer Settings	TWGCB-01-004-0181	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-33047-2
182	Windows8.1 Computer Settings	TWGCB-01-004-0182	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-33094-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
183	Windows8.1 Computer Settings	TWGCB-01-004-0183	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-33431-8
184	Windows8.1 Computer Settings	TWGCB-01-004-0184	使用者權限指派	建立權杖物件	▪這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	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-33779-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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			
185	Windows8.1 Computer Settings	TWGCB-01-004-0185	使用者權限指派	建立通用物件	▪這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-33095-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
186	Windows8.1 Computer Settings	TWGCB-01-004-0186	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-33780-8
187	Windows8.1 Computer Settings	TWGCB-01-004-0187	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： (1)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 (2)此設定可搭配 symlink file	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-33053-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
188	Windows8.1 Computer Settings	TWGCB-01-004-0188	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-33157-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
189	Windows8.1 Computer Settings	TWGCB-01-004-0189	使用者權限指派	拒絕從網路存取這台電腦	▪這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，則這項原則設定會取代「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-34173-5
190	Windows8.1 Computer Settings	TWGCB-01-004-0190	使用者權限指派	拒絕以批次工作登入	▪這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，則這項原則設定會取代「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-35461-3
191	Windows8.1	TWGC	使用者	拒絕以服	▪這項原則設定決定會阻止哪些	電腦設定	Guests	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0191	權限指派	務方式登入	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，則這項原則設定會取代「以服務方式登入」原則設定 ▪ 注意：這項原則設定不適用於 System、Local Service 或 Network Service 帳戶	\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		CCE-35404-3
192	Windows8.1 Computer Settings	TWGCB-01-004-0192	使用者權限指派	拒絕本機登入	▪ 這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，則這項原則設定會取代「允許本機登入」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\拒絕本機登入	Guests	CCE-ID：CCE-35293-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪注意：如果將此安全性原則套用到 Everyone 群組，將無人可登入本機			
193	Windows8.1 Computer Settings	TWGCB-01-004-0193	使用者權限指派	拒絕透過遠端桌面服務登入	▪這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 ▪注意：此設定對於尚未升級至 Service Pack2 的 Windows 2000 電腦沒有任何影響	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕透過遠端桌面服務登入	NT AUTHORITY\Local Account, Guests	CCE-ID：CCE-33787-3
194	Windows8.1 Computer Settings	TWGCB-01-004-0194	使用者權限指派	讓電腦及使用者帳戶受信賴，以進行委派	▪此安全性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	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	No one	CCE-ID：CCE-33778-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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。	進行委派		
195	Windows8.1	TWGC	使用者	強制從遠	▪ 這項原則設定決定哪些使用者	電腦設定	Administra	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0195	權限指派	端系統進行關閉	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	\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	tors	CCE-33715-4
196	Windows8.1 Computer Settings	TWGCB-01-004-0196	使用者權限指派	產生安全性稽核	▪這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-35363-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
197	Windows8.1 Computer Settings	TWGCB-01-004-0197	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-34021-6
198	Windows8.1 Computer Settings	TWGCB-01-004-0198	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	電腦設定\Windows 設定\安全性設定\本機原則\使用者	Administrators，Local Service	CCE-ID：CCE-34897-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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	權限指派\增加處理程序工作組		
199	Windows8.1 Computer Settings	TWGCB-01-004-0199	使用者權限指派	增加排程優先順序	▪這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	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-35178-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					面來變更處理程序的排程優先順序			
200	Windows8.1 Computer Settings	TWGCB-01-004-0200	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-34903-5
201	Windows8.1 Computer Settings	TWGCB-01-004-0201	使用者權限指派	存取認證管理員為信任呼叫者	▪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	電腦設定\Windows 設定\安全性設定\本機原則\使用	No one	CCE-ID：CCE-35457-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					其他實體，則使用者儲存的認證可能會被洩露	者權限指派\存取認證管理員為信任呼叫者		
202	Windows8.1 Computer Settings	TWGCB-01-004-0202	使用者權限指派	鎖定記憶體中的分頁	▪這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-33807-9
203	Windows8.1 Computer Settings	TWGCB-01-004-0203	使用者權限指派	以批次工作登入	▪這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	CCE-ID：CCE-33432-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
204	Windows8.1 Computer Settings	TWGCB-01-004-0204	使用者權限指派	以服務方式登入	▪這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-33731-1
205	Windows8.1 Computer Settings	TWGCB-01-004-0205	使用者權限指派	管理稽核及安全性記錄檔	▪這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 ▪這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	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-35275-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
206	Windows8.1 Computer Settings	TWGCB-01-004-0206	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-34913-4
207	Windows8.1 Computer	TWGCB-01-004-020	使用者權限指	修改韌體環境值	▪這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	電腦設定\Windows 設定\安全性設定\本	Administrators	CCE-ID：CCE-35183-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	7	派		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：這項原則設定不會影響	機原則\使用者權限指派\修改韌體環境值		3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
208	Windows8.1 Computer Settings	TWGCB-01-004-0208	使用者權限指派	執行磁碟區維護工作	▪這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-35369-8
209	Windows8.1 Computer Settings	TWGCB-01-004-0209	使用者權限指派	監視單一處理程序	▪這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	Administrators	CCE-ID：CCE-35000-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						單一處理程序		
210	Windows8.1 Computer Settings	TWGCB-01-004-0210	使用者權限指派	設定檔系統效能	▪這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\設定檔系統效能	Administrators，WdiServiceHost	CCE-ID：CCE-35001-7
211	Windows8.1 Computer Settings	TWGCB-01-004-0211	使用者權限指派	從銜接站移除電腦	▪這項原則設定決定使用者是否無需登入便可從銜接站卸除可攜式電腦 ▪如果啟用此原則，使用者必須先登入，才能從銜接站移除可攜式電腦 ▪如果停用此原則，使用者無需登入便可從銜接站移除可攜式電腦	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從銜接站移除電腦	Administrators，Users	CCE-ID：CCE-33720-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
212	Windows8.1 Computer Settings	TWGCB-01-004-0212	使用者權限指派	取代處理程序等級權杖	▪這項原則設定決定哪些使用者帳戶能夠呼叫 Create Process As User()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-35003-3
213	Windows8.1 Computer Settings	TWGCB-01-004-0213	使用者權限指派	還原檔案及目錄	▪這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：	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-35067-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(1)周遊資料夾/執行檔案 (2)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			
214	Windows8.1 Computer Settings	TWGCB-01-004-0214	使用者權限指派	關閉系統	▪這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-35004-1
215	Windows8.1 Computer Settings	TWGCB-01-004-021	使用者權限指派	取得檔案或其他物件的擁有	▪這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	電腦設定\Windows 設定\安全性設定\本	Administrators	CCE-ID：CCE-35009-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		5		權	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	機原則\使用者權限指派\取得檔案或其他物件的擁有權		
216	Windows8.1 Computer Settings	TWGCB-01-004-0216	本機原則\使用者權限指派	同步處理目錄服務資料	▪這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這項原則設定亦稱為 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	CCE-ID：CCE-35735-0
217	Windows8.1 Computer	TWGCB-01-0	本機原則\使	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	電腦設定\Windows 設定\	Administrators	CCE-ID：CCE-33051-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0217	用者權限指派		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」	安全性設定\本機原則\使用者權限指派\建立分頁檔		4
218	Windows8.1 Computer Settings	TWGCB-01-004-0218	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 8.1 ▪如果啟用這個原則設定，就不會執行精靈 ▪如果停用這個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 8.1\防止精靈執行	啟用	CCE-ID：CCE-35382-1
219	Windows8.1	TWGC	Windo	允許選用	▪這個原則設定可控制需要帳戶	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0219	ws 元件	Microsoft 帳戶	登入的 Windows 市集應用程式是否可以選用 Microsoft 帳戶。這個原則只會影響支援該功能的 Windows 市集應用程式 ▪ 如果啟用這個原則設定，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 ▪ 如果停用或未設定這個原則設定，則使用者必須使用 Microsoft 帳戶登入	管理範本\Windows 元件\應用程式執行階段\允許選用 Microsoft 帳戶		CCE-35803-6
220	Windows8.1 Computer Settings	TWGCB-01-004-0220	Windows 元件	關閉自動播放	▪ 這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	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：所有裝置	CCE-ID：CCE-33791-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					便會立即啟動 ▪如果啟用這項原則設定，即會停用光碟機及卸除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 ▪這個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，使用者就無法使用這個設定來啟用該功能 ▪注意：這個設定會同時出現在「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			
221	Windows8.1	TWGC	Windo	AutoRun	▪這個原則設定可設定 Auto Run	電腦設定\系統	啟用/不執	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0221	ws 元件	的預設行為	命令的預設行為 ▪ Auto Run 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 WindowsVista 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 WindowsVista 開始的預設行為是，提示使用者是否要執行 Auto Run 命令 ▪ Auto Run 命令會呈現為[自動播放]對話方塊中的處理常式 ▪ 如果啟用這個原則設定，系統	管理範本\Windows 元件\自動播放原則\AutoRun 的預設行為	行任何 Autorun 命令	CCE-34771-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					管理員可以將 WindowsVista 或更新版本的 Auto Run 預設行為變更為下列行為： -完全停用 Auto Run 命令，或者 -轉換回 Windows Vista 之前的行為，自動執行 Auto Run 命令 ▪ 如果停用或未設定這個原則設定，Windows Vista 或更新版本將會提示使用者是否要執行 Auto Run 命令			
222	Windows8.1 Computer Settings	TWGCB-01-004-0222	Windows 元件	不允許非磁碟區裝置的自動播放	▪ 這個原則設定不允許 MTP 裝置(如相機或電話)的自動播放 ▪ 如果啟用這個原則設定，將不允許 MTP 裝置(如相機或電話)的自動播放 ▪ 如果停用或未設定這個原則設定，將可啟用非磁碟區裝置的	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-35289-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					自動播放			
223	Windows8.1 Computer Settings	TWGCB-01-004-0223	Windows 元件	限制解壓縮和安裝未經數位簽署的小工具	▪ 這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 ▪ 如果啟用這項原則設定，未經過數位簽署的小工具不會解壓縮 ▪ 如果停用或未做這項原則設定，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數位簽署的小工具	啟用	CCE-ID：CCE-35559-4
224	Windows8.1 Computer Settings	TWGCB-01-004-0224	Windows 元件	關閉使用者安裝的桌面小工具	▪ 這個原則設定可讓關閉已由使用者安裝的桌面小工具 ▪ 如果啟用這個設定，Windows 不會執行任何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	啟用	CCE-ID：CCE-33254-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用或未設定這個設定，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	的桌面小工具		
225	Windows8.1 Computer Settings	TWGCB-01-004-0225	Windows 元件	關閉桌面小工具	▪這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 ▪如果啟用這項原則設定，將會關閉桌面小工具 ▪如果停用或未做這項原則設定，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-33140-5
226	Windows8.1 Computer Settings	TWGCB-01-004-0226	Windows 元件	Windows 錯誤報告	▪這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	電腦設定\系統管理範本\Windows 元件\Windows 錯誤	停用	CCE-ID：CCE-34245-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					「Windows 錯誤報告」事件將不會記錄到系統事件日誌	報告\停用記錄		
227	Windows8.1 Computer Settings	TWGCB-01-004-0227	Windows 元件	停用 Windows 錯誤報告	▪如果啟用這項原則設定，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	CCE-ID：CCE-34247-7
228	Windows8.1 Computer Settings	TWGCB-01-004-0228	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	CCE-ID：CCE-34527-2
229	Windows8.1 Computer	TWGCB-01-0	Windo	顯示錯誤	▪這個原則設定可以控制是否向使用者顯示讓他們報告錯誤的	電腦設定\系統管理範本	停用	CCE-ID：CCE-33735-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0229	ws 元件	通知	錯誤對話方塊 ▪如果啟用這個原則設定，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 ▪如果停用這個原則設定，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，停用這個原則設定很實用	\Windows 元件\Windows 錯誤報告\顯示錯誤通知		2
230	Windows8.1	TWGC	Windo	關閉	▪拒絕或允許存取此 Windows 郵	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0230	ws 元件	Windows 郵件應用程式	件應用程式 ▪ 如啟用這項設定，將拒絕存取 Windows 郵件應用程式 ▪ 如停用或不設定，將允許存取 Windows 郵件應用程式	管理範本\Windows 元件\Windows 郵件\關閉 Windows 郵件應用程式		CCE-33258-5
231	Windows8.1 Computer Settings	TWGCB-01-004-0231	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 郵件\關閉社群功能	啟用	CCE-ID：CCE-34063-8
232	Windows8.1 Computer Settings	TWGCB-01-004-0232	Windows 元件	永遠以較高的特殊權限安裝	▪ 這個原則設定會指定 Windows Installer 在安裝任何程式到系統時應使用較高的權限 ▪ 如果啟用這個原則設定，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	電腦設定\系統管理範本\Windows 元件\Windows Installer\永遠以較高的特殊權	停用	CCE-ID：CCE-35400-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 這個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) ▪ 如果停用或未設定這個原則設定，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：這個原則設定會同時出現在[電腦設定]及[使用者設	限安裝		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定]資料夾中。如果要讓這個原則設定生效，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這個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，這個原則設定的[使用者設定]版本不保證是安全的			
233	Windows8.1 Computer Settings	TWGCB-01-004-0233	Windows 元件	允許使用者控制安裝	▪ 這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 ▪ 這個設定不使用 Windows Installer 的某些安全性功能。它能讓安裝完成，不因安全性違規而暫停安裝	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-35431-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 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 ▪ 這個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			
234	Windows8.1	TWGC	Windo	禁止非系	▪ 這項原則設定控制非系統管理	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0234	ws 元件	統管理員套用廠商簽署的更新	員是否可以安裝已經由應用程式廠商數位簽署的更新 ▪如果啟用這項原則設定，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 ▪如果停用這項原則設定，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	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		CCE-32957-3
235	Windows8.1 Computer Settings	TWGCB-01-004-0235	Windows 元件	停用 Windows Installer 指令碼的 IE 安全性提示	▪這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	電腦設定\系統管理範本\Windows 元件\Windows Installer\停用 Windows Installer 指令碼	停用	CCE-ID：CCE-35086-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					裝。這個設定會抑制警告，並允許安裝繼續進行 ▪ 這個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企業所設計。不過，由於這個設定可能有安全性風險，因此應該謹慎使用	的 IE 安全性提示		
236	Windows8.1 Computer Settings	TWGCB-01-004-0236	Windows 元件	不要顯示「安裝第一次使用」對話方塊	▪ 這項原則設定決定是否要顯示「安裝第一次使用」對話方塊 ▪ 啟用這項原則時，在使用者第一次啟動 WindowsMediaPlayer 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這項原則，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-34706-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
237	Windows8.1 Computer Settings	TWGCB-01-004-0237	Windows 元件	防止自動更新	▪ 這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這項原則，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	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-34874-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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」，而且即使沒有這項原則，他們也不會看到更新提示			
238	Windows8.1 Computer Settings	TWGCB-01-004-0238	Windows 元件	不要顯示密碼顯示按鈕	▪這個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 ▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，當使用者在密碼輸入文字	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-32965-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪這個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 InternetExplorer			
239	Windows8.1 Computer Settings	TWGCB-01-004-0239	Windows 元件	提升權限時列舉系統管理員帳戶	▪這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	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-35194-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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			
240	Windows8.1 Computer Settings	TWGCB-01-004-0240	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)	▪如果啟用這個原則設定，且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 ▪如果停用或未設定這個原則設定，且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-34169-3
241	Windows8.1 Computer Settings	TWGCB-01-004-0241	Windows 元件	記錄檔大小上限(KB)(應用)	▪這項原則設定可決定記錄檔的大小上限(以 KB 為單位) ▪如果啟用這項原則設定，即可將記錄檔大小上限設定為介於	電腦設定\系統管理範本\Windows 元件\事件日誌服務\應用程式\記錄	啟用：32,768 KB	CCE-ID：CCE-33975-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					1MB(1024 KB)至2TB(2147483647 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	檔大小上限(KB)		
242	Windows8.1 Computer Settings	TWGCB-01-004-0242	Windows 元件	控制記錄檔達到其大小上限時的事件記錄檔行為(安全性)	▪如果啟用這個原則設定，且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 ▪如果停用或未設定這個原則設定，且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]	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-35090-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					原則設定所決定			
243	Windows8.1 Computer Settings	TWGCB-01-004-0243	Windows 元件	記錄檔大小上限(KB)(安全性)	▪這項原則設定決定記錄檔的大小上限(以 KB 為單位) ▪如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1MB(1024 KB)至 2TB(2147483647 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 20 MB	電腦設定\系統管理範本\Windows 元件\事件紀錄服務\安全性\記錄檔大小上限(KB)	啟用：81920 KB	CCE-ID：CCE-33428-4
244	Windows8.1 Computer	TWGCB-01-004-024	Windows 元件	記錄檔大小上限(KB)(安	▪這項原則設定決定記錄檔的大小上限(以 KB 為單位)	電腦設定\系統管理範本\Windows 元件\	啟用：32,768 KB	CCE-ID：CCE-35091-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	4		裝)	▪如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1MB(1024 KB)至 2TB(2147483647 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	事件紀錄服務\安裝\記錄檔大小上限(KB)		8
245	Windows8.1 Computer Settings	TWGCB-01-004-0245	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)	▪如果啟用這個原則設定，且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。 ▪如果停用或未設定這個原則設定，且記錄檔達到其大小上	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	停用	CCE-ID：CCE-33729-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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。	上限時的事件記錄檔行為		
246	Windows8.1 Computer Settings	TWGCB-01-004-0246	Windows 元件	記錄檔大小上限(KB)(系統)	▪這項原則設定決定記錄檔的大小上限(以 KB 為單位) ▪如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1024 KB)至 2 TB(2147483647 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 20 MB	電腦設定\系統管理範本\Windows 元件\事件紀錄服務\系統\記錄檔大小上限(KB)	啟用：32,768 KB	CCE-ID：CCE-35288-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
247	Windows8.1 Computer Settings	TWGCB-01-004-0247	Windows 元件	不允許儲存密碼	▪這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 如果啟用這項原則設定，「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 ▪如果停用或未做這項原則設定，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-34506-6
248	Windows8.1 Computer Settings	TWGCB-01-004-024	Windows 元件	允許使用者使用遠端桌面服	▪這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	電腦設定\系統管理範本\Windows 元件\	停用	CCE-ID：CCE-35255-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		8		務從遠端連線	▪如果啟用這項原則設定，目標電腦上隸屬於 RemoteDesktopUsers 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 ▪如果停用這項原則設定，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 ▪如果未設定這項原則設定，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		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
249	Windows8.1 Computer	TWGCB-01-0	Windo	不允許磁碟重新導	▪這個原則設定指定在遠端桌面服務工作階段中，是否要防止	電腦設定\系統管理範本	啟用	CCE-ID：CCE-34697-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0249	ws 元件	向	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。可以使用這個原則設定覆寫這種行為 ▪ 如果啟用這個原則設定，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，而且不允許在執行 Windows Server 2003、Windows 8 和 Windows XP 的電腦上，重新導向剪貼簿檔案複製	\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		3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用這個原則設定，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 ▪如果未設定這個原則設定，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			
250	Windows8.1 Computer Settings	TWGCB-01-004-0250	Windows 元件	連線時永遠提示密碼	▪這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 ▪使用者可以使用這項設定，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	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-33960-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果這項原則設定為「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 ▪ 如果這項原則設定為「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 ▪ 如果這項原則設定為「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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					作階段主機設定工具，強制執行密碼提示			
251	Windows8.1 Computer Settings	TWGCB-01-004-0251	Windows 元件	設定用戶端連線加密層級	▪這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 ▪如果啟用這項原則設定，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加密方法。加密層級預設為「高」。可用的加密方法如下： (1)高：設定「高」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	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-35578-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (2)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 (3)低：設定「低」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			
252	Windows8.1	TWGC	Windo	未使用中	▪這項原則設定決定使用中的遠	電腦設定\系統	啟用/15 分	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0252	ws 元件	但閒置的遠端桌面服務工作階段設定時間限制	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 ▪ 如果啟用這項原則設定，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 ▪ 如果停用或未設定這項原則設	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\未使用中但閒置的遠端桌面服務工作階段設定時間限制	鐘	CCE-35595-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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：這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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定，「電腦設定」原則具有較高的優先順序			
253	Windows8.1 Computer Settings	TWGCB-01-004-0253	Windows 元件	設定已斷線工作階段的時間限制	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用或未設定這項原則設定，已中斷連線的工作階段會無限期保留。使用者可以在遠	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-35599-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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：這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			
254	Windows8.1 Computer Settings	TWGCB-01-004-0254	Windows 元件	遠端桌面服務	▪這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 ▪如果狀態設定為「啟用」，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	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	停用	CCE-ID：CCE-34519-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果狀態設定為「停用」，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 ▪如果狀態設定為「尚未設定」，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：這個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	料夾		
255	Windows8.1	TWGC	Windo	不要使用	▪這項原則設定決定是否禁止遠	電腦設定\系統	停用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0255	ws 元件	每一工作階段的暫存資料夾	端桌面服務建立特定工作階段的暫存資料夾 ▪ 如果啟用這項原則設定，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 ▪ 如果停用這項原則設定，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 ▪ 如果未設定這項原則設定，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	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		CCE-34531-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					存資料夾			
256	Windows8.1 Computer Settings	TWGCB-01-004-0256	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]	▪這個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 ▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，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	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-34491-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					[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，則這個原則設定就無效			
257	Windows8.1 Computer Settings	TWGCB-01-004-0257	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 ▪啟用這個原則將停用該功能，也可能造成 Windows 市集這類公用服務的連線停止運作	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-33929-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪注意：這部電腦設定為使用「指定內部網路 Microsoft 更新服務位置」原則連線到內部網路更新服務時，才適用這個原則			
258	Windows8.1 Computer Settings	TWGCB-01-004-0258	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	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用或沒有進行這項原則設定，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	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-34520-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Windows」對話方塊中就會有「安裝更新並關機」選項可供使用			
259	Windows8.1 Computer Settings	TWGCB-01-004-0259	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	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用或未設定這項原則設定，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	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-33813-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
260	Windows8.1 Computer Settings	TWGCB-01-004-0260	Windows 元件	重新排程已經排程好的自動更新安裝	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用這項原則設定，錯過的排程安裝將會於下一個排程安裝同時發生 ▪如果尚未設定這項原則設定，錯過的排程安裝將會於下次開機後一分鐘發生	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-33027-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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			
261	Windows8.1 Computer Settings	TWGCB-01-004-0261	Windows 元件	設定自動更新	▪這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： (1)2=下載任何更新前通知我，並在安裝到我的電腦前再一次通知我：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。	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	CCE-ID：CCE-35111-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 (2)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 (3)4=自動下載更新，並於以下			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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)			
262	Windows8.1 Computer Settings	TWGCB-01-004-0262	Windows 元件	允許基本驗證	▪ 這個原則設定可管理 Windows 遠端管理(WinRM)用戶端是否使用基本驗證 ▪ 如果啟用這個原則設定，WinRM 用戶端會使用基本驗證。如果將 WinRM 設定為使用	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理(WinRM)\Win	停用	CCE-ID：CCE-35258-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					HTTP 傳輸，使用者名稱及密碼就會以純文字在網路上傳送 ▪如果停用或未設定這個原則設定，WinRM 用戶端不會使用基本驗證	RM 用戶端\允許基本驗證		
263	Windows8.1 Computer Settings	TWGCB-01-004-0263	Windows 元件	允許未加密的流量(用戶端)	▪這個原則設定可管理 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 ▪如果啟用這個原則設定，WinRM 用戶端會透過網路傳送和接收未加密的訊息 ▪如果停用或未設定這個原則設定，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-34458-0
264	Windows8.1	TWGC	Windo	不允許摘	▪這個原則設定可管理 Windows	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0264	ws 元件	要式驗證	遠端管理(WinRM)用戶端是否使用摘要式驗證 ▪如果啟用這個原則設定，WinRM 用戶端不會使用摘要式驗證 ▪如果停用或未設定這個原則設定，WinRM 用戶端會使用摘要式驗證	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		CCE-34778-1
265	Windows8.1 Computer Settings	TWGCB-01-004-0265	Windows 元件	允許未加密的流量(服務)	▪這個原則設定可管理 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 ▪如果啟用這個原則設定，WinRM 用戶端會透過網路傳送和接收未加密的訊息 ▪如果停用或未設定這個原則設定，WinRM 用戶端只會透過網	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-35054-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					路傳送或接收加密的訊息			
266	Windows8.1 Computer Settings	TWGCB-01-004-0266	Windows 元件	不允許 WinRM 儲存 RunAs 認證	▪ 這個原則設定可管理 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 ▪ 如果啟用這個原則設定，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 ▪ 如果停用或未設定這個原則設定，WinRM 服務將允許外掛程式設定 RunAsUser 和 RunAsPassword 設定值，而且	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-35416-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					可安全地儲存 RunAsPassword 值 ▪ 如果啟用後又停用這個原則設定，必須重設先前設定的所有 RunAsPassword 值			
267	Windows8.1 Computer Settings	TWGCB-01-004-0267	Windows 元件	設定 Windows Smart Screen 篩選工具	▪ 這個原則設定可管理 Windows Smart Screen 篩選工具的行為 ▪ Windows Smart Screen 篩選工具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 ▪ 如果啟用這個原則設定，可以透過設定下列其中一個選項來控制 Windows Smart Screen 篩	電腦設定\系統管理範本\Windows 元件\Windows 檔案總管\設定 Windows Smart Screen 篩選工具	啟用：在執行不明軟體下載之前需要系統管理員核准	CCE-ID：CCE-34026-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果停用或未設定這個原則設定，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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
268	Windows8.1 Computer Settings	TWGCB-01-004-0268	Windows 元件	關閉檔案總管的資料執行防止	▪這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\Windows 檔案總管\關閉檔案總管的資料執行防止	停用	CCE-ID：CCE-33608-1
269	Windows8.1 Computer Settings	TWGCB-01-004-0269	Windows 元件	損毀時關閉終止堆集	▪這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\Windows 檔案總管\損毀時關閉終止堆集	停用	CCE-ID：CCE-33745-1
270	Windows8.1 Computer Settings	TWGCB-01-004-0270	Windows 元件	關閉殼層通訊協定受保護模式	▪這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	電腦設定\系統管理範本\Windows 元件\Windows 檔案	停用	CCE-ID：CCE-33764-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪ 如果啟用這項原則設定，則會完整啟用通訊協定，允許開啟資料夾及檔案 ▪ 如果停用這項原則設定，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 ▪ 如果未設定這項原則設定，通訊協定將會處於受保護模式，	總管\關閉殼層通訊協定受保護模式		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					只允許應用程式開啟一組有限的資料夾			
271	Windows8.1 Computer Settings	TWGCB-01-004-0271	Windows 元件	關閉遊戲資訊下載	▪這項原則設定決定是否管理來自 Windows Metadata Services 之GameBox 圖片及評分的下載 ▪如果啟用此設定，則不會下載包含GameBox 圖片及評分的遊戲資訊 ▪如果停用或未設定此設定，則會從 WindowsMetadataServices 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	CCE-ID：CCE-35780-6
272	Windows8.1 Computer Settings	TWGCB-01-004-0272	Windows 元件	關閉遊戲更新	▪這項原則設定決定是否管理從 Windows Metadata Services 下載遊戲更新資訊 ▪如果啟用這項原則設定，將不會下載遊戲更新資訊	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	CCE-ID：CCE-33201-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用或未設定這個設定，則會從 WindowsMetadataServices 下載遊戲更新資訊			
273	Windows8.1 Computer Settings	TWGCB-01-004-0273	Windows 元件	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	▪這個原則設定可控制裝置是否在 WindowsUpdate 重新啟動系統之後自動登入最後一個互動式使用者 ▪如果啟用或未設定這個原則設定，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 WindowsUpdate 重新啟動之後設定自動登入 ▪WindowsUpdate 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	電腦設定\系統管理範本\Windows 元件\Windows 登入選項\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	停用	CCE-ID：CCE-33891-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					設定的所有鎖定畫面的應用程式鎖定 ▪如果停用這個原則設定，裝置不會儲存 WindowsUpdate 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			
274	Windows8.1 Computer Settings	TWGCB-01-004-0274	Windows 元件	於使用者登入期間，報告登入伺服器無法使用	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用或未設定這項原則設	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-33012-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定，則不會向使用者顯示任何快顯			
275	Windows8.1 Computer Settings	TWGCB-01-004-0275	Windows 元件	允許加密檔案索引	▪製索引 ▪如果啟用這項原則設定，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\允選加密檔案索引	停用	CCE-ID：CCE-35314-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
276	Windows8.1 Computer Settings	TWGCB-01-004-0276	Windows 元件	啟用為未快取之 Exchange 資料夾編製索引的功能	▪這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 ▪啟用這項原則可允許在 MicrosoftOutlook 不是以快取模式執行時，針對 MicrosoftExchange 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 ▪停用這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	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-35319-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					箱編製索引，必須同時停用這兩個原則			
277	Windows8.1 Computer Settings	TWGCB-01-004-0277	Windows 元件	防止電腦加入 Home Group	▪這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 Home Group ▪如果啟用這項原則設定，這部電腦上的使用者無法將這部電腦新增到 Home Group。這個設定不影響其他網路共用功能 ▪如果停用或未設定這項原則設定，則使用者可以將這部電腦新增到 Home Group。但是已加入網域的電腦上的資料不會與 Home Group 共用	電腦設定\系統管理範本\Windows 元件\HomeGroup\防止電腦加入 HomeGroup	啟用	CCE-ID：CCE-34776-5
278	Windows8.1 Computer	TWGCB-01-004-027	Windows 元件	關閉定位	▪這個原則設定會關閉這部電腦的定位功能	電腦設定\系統管理範本\Windows 元件\	啟用	CCE-ID：CCE-33743-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	8			▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，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	定位和感應器\關閉定位		6
279	Windows8.1 Computer Settings	TWGCB-01-004-0279	Windows 元件	關閉市集應用程式	▪拒絕或允許存取市集應用程式。 ▪如果啟用這個設定，將拒絕存取市集應用程式。必須能夠存取市集才能安裝應用程式更新。 ▪如果停用或未設定這個設定，將允許存取市集應用程式。	電腦設定\系統管理範本\Windows 元件\市集\關閉市集應用程式	啟用	CCE-ID：CCE-35811-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
280	Windows8.1 Computer Settings	TWGCB-01-004-0280	Windows 元件	允許基本驗證	▪這個原則設定可管理 Windows 遠端管理(WinRM)服務是否接受來自遠端用戶端的基本驗證 ▪如果啟用這個原則設定，WinRM 服務會接受來自遠端用戶端的基本驗證 ▪如果停用或未設定這個原則設定，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-34779-9
281	Windows8.1 Computer Settings	TWGCB-01-004-0281	Windows 元件	加入 Microsoft MAPS	▪這個原則設定可加入 Microsoft MAPS。Microsoft 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	電腦設定\系統管理範本\Windows 元件\Windows Defender\MAPS\加入 Microsoft MAPS	停用	CCE-ID：CCE-33833-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪如果啟用這個設定，將以指定的成員資格加入 Microsoft MAPS ▪如果停用或未設定這個設定，使用者將不會加入 Microsoft MAPS			
282	Windows8.1	TWGC	Windo	防止	▪這項原則設定決定是否防止	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	B-01-004-0282	ws 元件	Windows Media DRM 網路網路存取	Windows Media Digital Rights Management(DRM)存取網際網路(或內部網路) ▪ 如果啟用這項原則設定，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這項原則設定時，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	管理範本\Windows 元件\Windows Media Digital Rights Management\防止 Windows Media DRM 網路網路存取		CCE-34886-2
283	Windows8.1 Computer Settings	TWGCB-01-004-0283	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	啟用	CCE-ID：CCE-34011-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						用遠端桌面共用		
284	Windows8.1 Computer Settings	TWGCB-01-004-0284	Windows 元件	關閉自動下載隨函附件	▪這個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 ▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，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-34822-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
285	Windows8.1 Computer Settings	TWGCB-01-004-0285	Windows 元件	不允許執行數位購物服務區	▪這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 Market place 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 Market place 數位購物服務區」 ▪如果啟用這項原則設定，「數位購物服務區」將不會執行 ▪如果停用或未設定這項原則設定，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-34497-8
286	Windows8.1 Computer Settings	TWGCB-01-004-028	Windows 元件	關閉清查收集器	▪這個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	電腦設定\系統管理範本\Windows 元件\	啟用	CCE-ID：CCE-34966-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		6			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 ▪如果啟用這個原則設定，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 ▪如果停用或未設定這個原則設定，則會開啟清查收集器 ▪注意：如果關閉客戶經驗改進計畫，這個原則設定將不會發生任何作用。清查收集器將會被關閉	應用程式相容性\關閉清查收集器		
287	Windows8.1 Computer	TWGCB-01-0	印表機	指向並列印限制	▪這個原則設定會控制用戶端的「指向並列印」行為，包括	電腦設定\系統管理範本\印表	啟用 使用者只	CCE-ID：CCE-33742-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0287			Windows Vista 電腦的安全性提示。這個原則設定只適用於非列印系統管理員的用戶端，以及屬於網域成員的電腦 ▪ 如果啟用這個原則設定： -WindowsXP 和更新版本的用戶端只會從明確命名的伺服器清單下載列印驅動程式元件。如果用戶端有相容的列印驅動程式，就會建立印表機連線。如果用戶端上無法使用相容的列印驅動程式，則不會建立任何連線 -可以設定 WindowsVista 用戶端，在使用者指向並列印時，或必須更新印表機連線的驅動程式時，不顯示安全性警告和	機\指向並列印限制	能指向並列印所在樹系內的電腦	8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					提升權限的命令提示 ▪ 如果未設定這個原則設定： -WindowsVista 用戶端電腦可以指向並列印到任何伺服器 -當使用者使用指向並列印來建立與任何伺服器的印表機連線時，WindowsVista 電腦會顯示警告和提升權限的命令提示 -必須更新現有印表機連線的驅動程式時，WindowsVista 電腦會顯示警告和提升權限的命令提示 -WindowsServer2003 和 WindowsXP 用戶端電腦可以使用指向並列印來建立與所在樹系中任何伺服器的印表機連線 ▪ 如果停用這個原則設定：			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					-WindowsVista 用戶端電腦可以使用指向並列印來建立與任何伺服器的印表機連線。 -當使用者使用指向並列印來建立與任何伺服器的印表機連線時，Windows Vista 電腦不會顯示警告和提升權限的命令提示 -必須更新現有印表機連線的驅動程式時，Windows Vista 電腦不會顯示警告和提升權限的命令提示 -Windows Server 2003 和 Windows XP 用戶端電腦可以使用指向並列印來建立與任何伺服器的印表機連線 -「使用者只能指向並列印所在樹系內的電腦」設定只會套用			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					到 Windows Server 2003 和 Windows XP SP1(及更新的 Service Pack)			
288	Windows8.1 Computer Settings	TWGCB-01-004-0288	印表機	擴充指向並列印連線以搜尋 Windows Update	▪這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 ▪如果啟用這項原則設定，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 ▪如果停用這項原則設定，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	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-34752-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					式，則指向並列印連線會失敗			
289	Windows8.1 User Settings	TWGCB-01-004-0289	附件管理員	不要保留檔案附件的區域資訊	▪這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 ▪如果啟用這項原則設定，Windows 就不會標示附件檔案的區域資訊 ▪如果停用這項原則設定，Windows 就會標示附件檔案的區域資訊 ▪如果不設定這項原則設定，	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-34810-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Windows 就會標示附件檔案的區域資訊			
290	Windows8.1 User Settings	TWGCB-01-004-0290	附件管理員	隱藏移除區域資訊的機制	▪ 這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 ▪ 如果啟用這項原則設定，Windows 會隱藏核取方塊以及「解除封鎖」按鈕 ▪ 如果停用這項原則設定，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-34095-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果不設定這項原則設定，Windows 會顯示核取方塊以及「解除封鎖」按鈕			
291	Windows8.1 User Settings	TWGCB-01-004-0291	附件管理員	開啟附件時通知防毒程式	▪這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	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-33799-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
292	Windows8.1 User Settings	TWGCB-01-004-0292	網路共用	防止使用者共用其設定檔內的檔案	▪這個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 ▪如果啟用這個原則設定，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，	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-33490-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪如果停用或未設定這個原則設定，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			
293	Windows8.1 User Settings	TWGCB-01-004-0293	網際網路通訊設定	關閉說明分級	▪這項原則設定決定使用者是否可以提供說明內容分級 ▪若啟用這項原則設定，則會禁止在說明內容中加入分級控制 ▪若停用或未設定這項原則設定，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	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-35589-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					實用性的意見回饋			
294	Windows8.1 User Settings	TWGCB-01-004-0294	個人化	啟用螢幕保護裝置	▪這項原則設定決定是否啟用桌面螢幕保護裝置 ▪如果啟用這項原則設定，只要下列兩個條件成立，螢幕保護裝置就會執行： (1)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 (2)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 如果停用這個設定，螢幕保護裝置不會執行。此外，這個設定會停用「個人化」或「顯示」控制台中的「螢幕保護裝置」	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-33164-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪如果未做這個設定，這個設定對系統沒有作用			
295	Windows8.1 User Settings	TWGCB-01-004-0295	個人化	以密碼保護螢幕保護裝置	▪這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 ▪如果啟用這項原則設定，所有螢幕保護裝置都會受到密碼保護 ▪如果停用這個設定，則無法在任何螢幕保護裝置上設定密碼保護 這個設定也會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的「受密	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-32938-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					碼保護」核取方塊，以防止使用者變更密碼保護設定 ▪如果未做這個設定，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			
296	Windows8.1 User Settings	TWGCB-01-004-0296	個人化	螢幕保護裝置逾時	▪這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	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	CCE-ID：CCE-33168-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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，這個設定沒有作用： (1)設定已停用或未設定 (2)等候時間設為零 (3)「啟用螢幕保護裝置」設定已停用 (4)「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			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					「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			
297	Windows8.1 User Settings	TWGCB-01-004-0297	個人化	強制特定的螢幕保護裝置	▪如果啟用這個設定，系統會在使用者的桌面上顯示指定的螢幕保護裝置。此外，這個設定會停用[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 ▪如果停用或未設定這個設定，則使用者可以選取任一螢幕保護裝置 ▪如果啟用這個設定，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	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-33105-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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這個設定的電腦上，就會略過這個設定 ▪注意：這個設定可能已被「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，就會略過這個設定，而且螢幕保護裝置不會執行			
298	Windows8.1 User Settings	TWGCB-01-004-0298	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 ▪這個設定會防止使用者利用[控制台]新增、設定或變更電腦	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-33642-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					上的螢幕保護裝置。但這個設定不會防止螢幕保護裝置執行			
299	Windows8.1 User Settings	TWGCB-01-004-0299	其他	在鎖定畫面上關閉快顯通知	▪這個原則設定可在鎖定畫面上關閉快顯通知 ▪如果啟用這個原則設定，應用程式將無法在鎖定畫面上引發快顯通知 ▪如果停用或未設定這個原則設定，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。這個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-33727-9
300	Windows8.1 User Settings	TWGCB-01-004-030	Windows 元件	傳真服務	▪這個原則設定會允許或禁止使用這個嵌入式管理單元 ▪如果啟用這個原則設定，就會	使用者設定\系統管理範本\Windows 元件\Microsoft	停用	CCE-ID：CCE-35129-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		0			允許使用嵌入式管理單元，而且可以將它新增至 Microsoft Management Console 或從命令列執行做為獨立主控台 ▪如果停用這個原則設定，就會禁止使用嵌入式管理單元，而且不能將它新增至 Microsoft Management Console 或從命令列執行做為獨立主控台。錯誤訊息隨即顯示，並說明原則禁止使用這個嵌入式管理單元 ▪如果未設定這個原則設定，便由[限制使用者只能使用明確許可的嵌入式管理單元清單]設定決定允許或禁止使用此嵌入式管理單元 ▪如果已啟用[限制使用者只能	Management Console\限制的/許可的嵌入式管理單元\傳真服務		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					使用明確允許的嵌入式管理單元清單]原則設定，除了已經明確允許的嵌入式管理單元之外，使用者將無法使用任何其他的嵌入式管理單元。若要明確許可使用這個嵌入式管理單元，請啟用這個原則設定。如果未設定或停用這個原則設定，將禁止使用這個嵌入式管理單元 ▪ 如果已停用或未設定[限制使用者只能使用明確允許的嵌入式管理單元清單]原則設定，除了已經明確禁止的嵌入式管理單元之外，使用者將可以使用任何其他的嵌入式管理單元。若要明確禁止使用這個嵌入式管理單元，請停用這個原則設			

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定 ▪如果未設定或啟用這個原則設定，將允許使用這個嵌入式管理單元 ▪當某個嵌入式管理單元禁止使用時，它將不會出現在 MMC 的[新增/移除嵌入式管理單元]視窗中。此外，當使用者開啟包含禁止使用的嵌入式管理單元的主控台檔案時，該主控台檔案會開啟，但不會出現禁止使用的嵌入式管理單元			
301	Windows8.1 User Settings	TWGCB-01-004-0301	Windows 元件	防止轉碼器下載	▪這個原則設定可防止 Windows Media Player 下載轉碼器 ▪如果啟用這個原則設定，會防止 Player 自動將轉碼器下載至使用者的電腦。此外，Player	使用者設定\系統管理範本\Windows 元件\Windows Media Player\	啟用	CCE-ID：CCE-33793-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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 ▪如果停用這個原則設定，轉碼器會自動下載，且無法使用[自動下載轉碼器]核取方塊 ▪如果未設定這個原則設定，使用者可以變更[自動下載轉碼器]核取方塊的設定	播放\防止轉碼器下載		
302	Windows8.1 Firewall Settings	TWGCB-01-004-0302	具有進階安全性的Windows 防火牆	Windows 防火牆：禁止通知(網域)	▪這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 ▪如果啟用這項原則設定，Windows 防火牆將禁止顯示這些通知	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	CCE-ID：CCE-33062-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用這項原則設定，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 ▪如果未設定這項原則設定，Windows 防火牆會當作已停用這項原則設定，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			
303	Windows8.1	TWGC	具有進	Windows	▪這項原則設定決定是否禁止此	電腦設定\系統	啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Firewall Settings	B-01-004-0303	階安全性的Windows 防火牆	防火牆：禁止單點傳送回應到多點傳送或廣播要求(網域)	電腦接收其傳出之多點傳送或廣播訊息的單點傳送回應 ▪ 如果啟用這項原則設定，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 ▪ 如果停用或沒有進行這項原則設定，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。	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		CCE-33060-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
304	Windows8.1 Firewall Settings	TWGCB-01-004-0304	具有進階安全性的 Windows 防火牆	套用本機防火牆規則(網域)	▪這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	CCE-ID：CCE-33061-3
305	Windows8.1 Firewall Settings	TWGCB-01-004-0305	具有進階安全性的 Windo	套用本機連線安全性規則(網域)	▪這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	否	CCE-ID：CCE-35701-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			ws 防火牆			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		
306	Windows8.1 Firewall Settings	TWGCB-01-004-0306	具有進階安全性的 Windows 防火牆	輸出連線(網域)	▪ 這項原則設定決定 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)	CCE-ID：CCE-33098-5
307	Windows8.1 Firewall Settings	TWGCB-01-004-030	具有進階安全性的	輸入連線(網域)	▪ 這項原則設定決定 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	封鎖(預設)	CCE-ID：CCE-33063-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		7	Windows 防火牆			有進階安全性的 Windows 防火牆\內容\網域設定檔\輸入連線		
308	Windows8.1 Firewall Settings	TWGCB-01-004-0308	具有進階安全性的 Windows 防火牆	記錄丟棄的封包 (網域)	▪ 這項原則設定決定 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	CCE-ID：CCE-35252-6
309	Windows8.1 Firewall Settings	TWGCB-01-004-0309	具有進階安全性的 Windo	記錄成功的連線 (網域)	▪ 這項原則設定決定 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	是	CCE-ID：CCE-35306-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			ws 防火牆			的 Windows 防火牆\內容\網域設定檔\記錄\記錄成功的連線		
310	Windows8.1 Firewall Settings	TWGCB-01-004-0310	具有進階安全性的 Windows 防火牆	大小限制(網域)	▪ 這項原則設定決定 Windows 防火牆記錄檔的大小	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	16384	CCE-ID：CCE-35083-5
311	Windows8.1 Firewall Settings	TWGCB-01-004-0311	具有進階安全性的 Windows 防火	名稱(網域)	▪ 這項原則設定決定 Windows 防火牆記錄檔的名稱	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防	%windir%\system32\logfiles\firewall\domainfirewall	CCE-ID：CCE-34176-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			牆			火牆\內容\網域設定檔\記錄\名稱	.log	
312	Windows8.1 Firewall Settings	TWGCB-01-004-0312	具有進階安全性的 Windows 防火牆	防火牆狀態(網域)	▪ 這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)	CCE-ID：CCE-33160-3
313	Windows8.1 Firewall Settings	TWGCB-01-004-0313	具有進階安全性的 Windows 防火牆	顯示通知(私人)	▪ 這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	是(預設)	CCE-ID：CCE-33065-4

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						設定檔\自訂\防火牆設定\顯示通知		
314	Windows8.1 Firewall Settings	TWGCB-01-004-0314	具有進階安全性的 Windows 防火牆	允許單點傳播回應 (私人)	▪ 這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 ▪ 如果啟用這項原則設定，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 ▪ 如果停用或沒有進行這項原則設定，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	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	CCE-ID：CCE-35536-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪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			
315	Windows8.1 Firewall Settings	TWGCB-01-004-0315	具有進階安全性的 Windows 防火牆	套用本機防火牆規則(私人)	▪這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	CCE-ID：CCE-35702-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
316	Windows8.1 Firewall Settings	TWGCB-01-004-0316	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)	▪這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	CCE-ID：CCE-33064-7
317	Windows8.1 Firewall Settings	TWGCB-01-004-0317	具有進階安全性的 Windows 防火牆	防火牆狀態(私人)	▪這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	開啟(建議選項)	CCE-ID：CCE-33066-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						狀態		
318	Windows8.1 Firewall Settings	TWGCB-01-004-0318	具有進階安全性的 Windows 防火牆	輸出連線(私人)	▪ 這項原則設定決定 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)	CCE-ID：CCE-33162-9
319	Windows8.1 Firewall Settings	TWGCB-01-004-0319	具有進階安全性的 Windows 防火牆	輸入連線(私人)	▪ 這項原則設定決定 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)	CCE-ID：CCE-33161-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
320	Windows8.1 Firewall Settings	TWGCB-01-004-0320	具有進階安全性的 Windows 防火牆	名稱(私人)	▪ 這項原則設定決定 Windows 防火牆記錄檔的名稱	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	CCE-ID：CCE-33437-5
321	Windows8.1 Firewall Settings	TWGCB-01-004-0321	具有進階安全性的 Windows 防火牆	大小限制(私人)	▪ 這項原則設定決定 Windows 防火牆記錄檔的大小	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	16384	CCE-ID：CCE-34356-6
322	Windows8.1	TWGC	具有進	記錄丟棄	▪ 這項原則設定決定 Windows 防	電腦設定	是	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Firewall Settings	B-01-004-0322	階安全性的Windows 防火牆	的封包(私人)	火牆是否記錄丟棄的封包	\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		CCE-33436-7
323	Windows8.1 Firewall Settings	TWGCB-01-004-0323	具有進階安全性的Windows 防火牆	記錄成功的連線(私人)	▪ 這項原則設定決定 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	CCE-ID：CCE-34177-6
324	Windows8.1 Firewall	TWGCB-01-0	具有進階安全	顯示通知(公用)	▪ 這項原則設定決定當程式因為接收輸入連線而被封鎖時，是	電腦設定\Windows 設定\	是	CCE-ID：CCE-33068-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	04-0324	性的Windows 防火牆		否為使用者顯示通知	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		8
325	Windows8.1 Firewall Settings	TWGCB-01-004-0325	具有進階安全性的Windows 防火牆	允許單點傳播回應(公用)	▪ 這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 ▪ 如果啟用這項原則設定，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 ▪ 如果停用或沒有進行這項原則設定，且這部電腦將多點傳送	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	CCE-ID：CCE-33067-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					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			
326	Windows8.1 Firewall Settings	TWGCB-01-004-0326	具有進階安全性的 Windows 防火	套用本機防火牆規則(公用)	▪ 這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	否	CCE-ID：CCE-35537-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			牆			火牆\內容\公用設定檔\自訂\規則合併\套用本機防火牆規則		
327	Windows8.1 Firewall Settings	TWGCB-01-004-0327	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)	▪這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	CCE-ID：CCE-33099-3
328	Windows8.1 Firewall Settings	TWGCB-01-004-032	具有進階安全性的	防火牆狀態(公用)	▪這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	開啟(建議選項)	CCE-ID：CCE-35703-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
		8	Windows 防火牆			有進階安全性的 Windows 防火牆\內容\公用設定檔\防火牆狀態		
329	Windows8.1 Firewall Settings	TWGCB-01-004-0329	具有進階安全性的 Windows 防火牆	輸出連線(公用)	▪ 這項原則設定決定 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)	CCE-ID：CCE-33070-4
330	Windows8.1 Firewall Settings	TWGCB-01-004-0330	具有進階安全性的 Windo	輸入連線(公用)	▪ 這項原則設定決定 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	封鎖(預設)	CCE-ID：CCE-33069-6

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			ws 防火牆			的 Windows 防火牆\內容\公用設定檔\輸入連線		
331	Windows8.1 Firewall Settings	TWGCB-01-004-0331	具有進階安全性的 Windows 防火牆	大小限制(公用)	▪ 這項原則設定決定 Windows 防火牆記錄檔的大小	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	CCE-ID：CCE-35421-7
332	Windows8.1 Firewall Settings	TWGCB-01-004-0332	具有進階安全性的 Windows 防火	記錄丟棄的封包(公用)	▪ 這項原則設定決定 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	是	CCE-ID：CCE-35116-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			牆			火牆\內容\公用設定檔\記錄\記錄丟棄的封包		
333	Windows8.1 Firewall Settings	TWGCB-01-004-0333	具有進階安全性的 Windows 防火牆	記錄成功的連線(公用)	▪這項原則設定決定 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	CCE-ID：CCE-33734-5
334	Windows8.1 Firewall Settings	TWGCB-01-004-0334	具有進階安全性的 Windows 防火牆	名稱(公用)	▪這項原則設定決定 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	%windir%\system32\logfiles\firewall\publicfirewall.log	CCE-ID：CCE-35117-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						設定檔\記錄\名稱		

資料來源：本中心整理

參、 參考文獻

[1]Common Configuration Enumeration(CCE)List. http://cce.mitre.org/lists/cce_list.html

[2]CIS Security Benchmarks. https://benchmarks.cisecurity.org

[3]Windows 8.1 Security Guide, Version 1.0. Microsoft Security Compliance Manager. https://technet.microsoft.com/zh-tw/library/cc677002.aspx

[4]Microsoft Windows 8/8.1 Security Technical Implementation Guide Version:1 Release:8. http://iase.disa.mil/stigs/os/windows/Pages/win8.aspx

肆、 附件

附件 1 版次 1.7 異動設定項目列表

附件1 版次 1.7 異動設定項目列表

●刪除列表

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	Windows8.1 Computer Energy Settings	TWGCB-01-004-0335	電源管理\視訊與顯示設定	關閉顯示器(使用電池)	▪使用電池情況下，指定 Windows 關閉顯示器前的閒置時間 ▪如果啟用此原則，則必須提供 1 個以秒為單位之數值，指出應經過多長的閒置時間，Windows 才會關閉顯示器	電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定\關閉顯示器(使用電池)	啟用 1200(秒)
2	Windows8.1 Computer Energy Settings	TWGCB-01-004-0336	電源管理\視訊與顯示設定	關閉顯示器(使用一般電源)	▪使用一般電源情況下，指定 Windows 關閉顯示器前的閒置時間 ▪如果啟用此原則，則必須提供 1 個以秒為單位之數值，指出應經過多長的閒置時間，Windows 才會關閉顯示器	電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定\關閉顯示器(使用一般電源)	啟用 1200(秒)
3	Windows8.1	TWGCB	電源管理\	指定系統	▪這個原則設定可指定 Windows 轉換	電腦設定\系統範本	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Computer Energy Settings	-01-004-0337	睡眠設定	休眠逾時(使用電池)	系統為休眠前的閒置時間 ▪如啟用這個原則設定，使用者必須輸入數值(以秒為單位)，指出應經過多長的閒置時間，Windows 才會轉換為休眠 ▪如果停用或未設定這個原則設定，使用者可控制這個設定 ▪如果使用者設定電腦鎖定時在鎖定畫面上執行投影片放映，這可防止睡眠轉換。「防止啟用鎖定畫面投影片放映」原則設定也可以用來停用投影片放映功能。	設定\系統\電源管理\睡眠設定\指定系統休眠逾時(使用電池)	3600(秒)
4	Windows8.1 Computer Energy Settings	TWGCB-01-004-0338	電源管理\睡眠設定	指定系統休眠逾時(使用一般電源)	▪這個原則設定可指定 Windows 轉換系統為休眠前的閒置時間 ▪如果啟用這個原則設定，必須輸入數值(以秒為單位)，指出應經過多長的閒置時間，Windows 才會轉換為	電腦設定\系統範本設定\系統\電源管理\睡眠設定\指定系統休眠逾時(使用一般電源)	啟用 3600(秒)

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					休眠。 ▪如果停用或未設定這個原則設定，使用者可控制這個設定 ▪如果使用者設定電腦鎖定時在鎖定畫面上執行投影片放映，這可防止睡眠轉換。「防止啟用鎖定畫面投影片放映」原則設定也可以用來停用投影片放映功能。		
5	Windows8.1 Computer Settings	TWGCB-01-004-0339	安全性選項\互動式登入	互動式登入：給登入使用者的訊息本文	▪這項原則設定指定使用者登入時顯示的文字訊息 ▪此文字通常在合法動機下使用，例如，對誤用公司資訊的使用者提出警告，或警告使用者的動作可能會被稽核	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：給登入使用者的訊息本文	(請機關自行設計)
6	Windows8.1 Computer	TWGCB-01-004-	安全性選項\互動式	互動式登入：給登	▪這項原則設定允許在包含「互動式登入：給登入使用者的訊息本文」	電腦設定\Windows 設定\安全性設定\本	(請機關自行設

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings	0340	登入	入使用者的訊息標題	的視窗標題列顯示指定的標題	機原則\安全性選項\互動式登入：給登入使用者的訊息標題	計)

資料來源：本中心整理