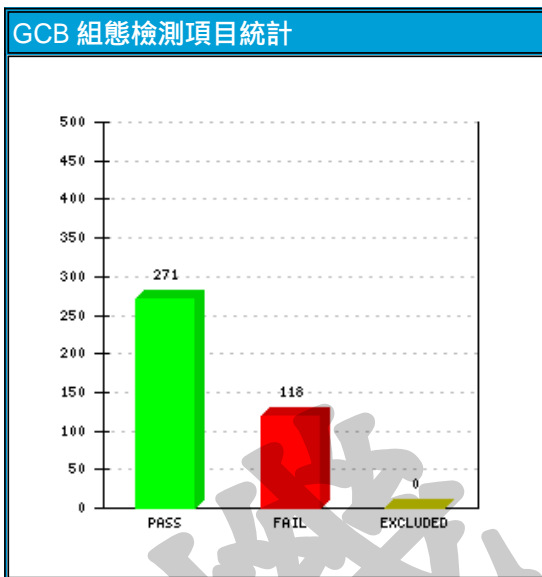


192.168.2.178 : WIN-7x32-MBP7

開始時間: 2015/08/17 12:56:29 - 2015/08/17 12:58:58
 作業系統: Windows 7 Professional Service Pack 1
 MAC / 開道: 00-1C-42-4F-2D-08
 MAC 供應商: 2 Parallels, Inc.
 電腦名稱: Windows 7 Professional Service Pack 1
 使用者帳號: SYSTEM
 CPU 規格: Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
 RAM 規格: 2,816 MBytes
 IE 版本: IE9, Update:11.0.20 (KB3058515), Version:11.0.9600.17843
 防毒軟體名稱: Microsoft Security Essentials



檢測摘要

編號	群組	合格	不合格	已排除	Total
1	Account Policy	1	1	0	2
2	Computer Energy Policy	4	0	0	4
3	Computer Settings	211	14	0	225
4	User Settings	8	0	0	8
5	Firewall Settings	34	1	0	35
6	Internet Explorer	13	102	0	115

規則摘要

Account Policy		FAIL
1 - 4	密碼必須符合複雜性需求 CCE-9370-8	FAIL
1 - 6	使用可還原的加密來存放密碼 CCE-9260-1	PASS
Computer Energy Policy		PASS

2 - 10	關閉顯示器(使用電池) CCE-12924-7	PASS
2 - 11	關閉顯示器(使用一般電源) CCE-12393-5	PASS
2 - 12	指定系統休眠逾時(使用電池) CCE-13091-4	PASS
2 - 13	指定系統休眠逾時(使用一般電源) CCE-13668-9	PASS

Computer Settings		FAIL
3 - 14	網路安全性：強制限制登入時數 CCE-9704-8	PASS
3 - 15	帳戶：重新命名系統管理員帳戶 CCE-8484-8	PASS
3 - 16	帳戶：重新命名來賓帳戶名稱 CCE-9229-6	PASS
3 - 17	網路存取：允許匿名 SID 名稱轉譯 CCE-9531-5	PASS
3 - 18	帳戶：Administrator 帳戶狀態 CCE-9199-1	PASS
3 - 19	帳戶：Guest 帳戶狀態 CCE-8714-8	PASS
3 - 20	修復主控台：允許自動系統管理登入 CCE-8807-0	PASS
3 - 21	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 CCE-8945-8	PASS
3 - 22	裝置：CD-ROM 存取只限於登入本機的使用者 CCE-9304-7	PASS
3 - 23	裝置：軟碟機存取只限於登入本機的使用者 CCE-9440-9	PASS
3 - 24	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 CCE-8487-1	PASS
3 - 25	互動式登入：要求網域控制站驗證以解除鎖定工作站 CCE-8818-7	PASS
3 - 26	互動式登入：在密碼到期前提示使用者變更密碼 CCE-9307-0	PASS
3 - 27	互動式登入：智慧卡移除操作 CCE-9067-0	PASS
3 - 28	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 CCE-8958-1	PASS
3 - 29	使用者帳戶控制：標準使用者之提升權限提示的行為 CCE-8813-8	FAIL
3 - 30	互動式登入：不要要求按 CTRL+ALT+DEL 鍵 CCE-9317-9	FAIL
3 - 31	互動式登入：不要顯示上次登入的使用者名稱 CCE-9449-0	PASS
3 - 32	使用者帳戶控制：偵測應用程式安裝，並提示提升權限 CCE-9616-4	PASS
3 - 33	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-9189-2	PASS
3 - 34	使用者帳戶控制：僅針對在安全位置安裝的 UIAccess 應用程式，提高其權限 CCE-9189-2	PASS
3 - 35	使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置 CCE-8817-9	PASS
3 - 36	使用者帳戶控制：使用內建的 Administrator 帳戶的管理員核准模式 CCE-8817-9	PASS
3 - 37	網路安全性：設定 Kerberos 允許的加密類型 CCE-9532-3	PASS
3 - 38	互動式登入：給登入使用者的訊息標題 CCE-8740-3	PASS
3 - 39	互動式登入：給登入使用者的訊息本文 CCE-8973-0	PASS
3 - 40	使用者帳戶控制：提示提升權限時切換到安全桌面 CCE-9395-5	PASS
3 - 41	關機：允許不登入就將系統關機 CCE-9707-1	PASS
3 - 42	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 CCE-9021-7	PASS
3 - 43	稽核：稽核通用系統物件的存取 CCE-9150-4	PASS
3 - 44	網路存取：不允許存放網路驗證的密碼與認證 CCE-8654-6	PASS

3 - 45	網路存取：讓 Everyone 權限套用到匿名使用者 CCE-8936-7	PASS
3 - 46	系統加密編譯：Use FIPS 140 相容加密演算法，包括加密、雜湊以及簽署演算法 CCE-9266-8	PASS
3 - 47	網路存取：共用和安全性模式用於本機帳戶 CCE-9503-4	PASS
3 - 48	稽核：稽核備份與還原權限的使用 CCE-8789-0	PASS
3 - 49	帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 CCE-9418-5	PASS
3 - 50	網路安全性：LAN Manager 驗證等級 CCE-9503-4	PASS
3 - 51	網路安全性：允許 LocalSystem NULL 工作階段回復 CCE-8804-7	PASS
3 - 52	網路安全性：NTLM SSP 為主的(包含安全 RPC)用戶端的最小工作階段安全性 CCE-9534-9	PASS
3 - 53	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 CCE-9736-0	PASS
3 - 54	網路安全性：下次密碼變更時不儲存 LAN Manager 原則設定名稱 CCE-8937-5	PASS
3 - 55	網路安全性：允許對此電腦的 PKU2U 驗證要求原則設定名稱 CCE-9770-9	PASS
3 - 56	網路存取：不允許 SAM 帳戶和共用的匿名列舉 CCE-9156-1	PASS
3 - 57	網路存取：不允許 SAM 帳戶的匿名列舉 CCE-9249-4	PASS
3 - 58	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 CCE-9432-6	PASS
3 - 59	網路安全性：允許 Local System 對 NTLM 使用電腦身分識別 CCE-9096-9	PASS
3 - 60	裝置：防止使用者安裝印表機驅動程式 CCE-9026-6	PASS
3 - 61	網路存取：可遠端存取的登錄路徑 CCE-9121-5	PASS
3 - 62	網路存取：可遠端存取的登錄路徑及子路徑 CCE-9386-4	FAIL
3 - 63	系統物件：要求不區分大小寫用於非 Windows 子系統 CCE-9319-5	PASS
3 - 64	系統物件：加強內部系統物件的預設權限(例如：符號連結) CCE-9191-8	PASS
3 - 65	Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間 CCE-9406-0	PASS
3 - 66	網路伺服器：當登入時數到期時，中斷用戶端連線 CCE-9358-3	PASS
3 - 67	Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意) CCE-8825-2	PASS
3 - 68	網路存取：可以匿名存取的具名管道 CCE-9218-9	PASS
3 - 69	網路存取：可以匿名存取的共用 CCE-9196-7	PASS
3 - 70	Microsoft 網路伺服器：數位簽章伺服器的通訊(自動) CCE-9040-7	PASS
3 - 71	網路存取：限制匿名存取具名管道和共用 CCE-9540-6	PASS
3 - 72	Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級 CCE-8503-5	PASS
3 - 73	Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器 CCE-9265-0	PASS
3 - 74	Microsoft 網路伺服器：數位簽章用戶端的通訊(如果伺服器同意) CCE-9344-3	PASS
3 - 75	Microsoft 網路用戶端：數位簽章用戶端的通訊(自動) CCE-9327-8	PASS
3 - 76	網路安全性：LDAP用戶端簽章要求 CCE-9768-3	PASS
3 - 77	網域成員：停用電腦帳戶密碼變更 CCE-9295-7	PASS
3 - 78	網域成員：最長電腦帳戶密碼有效期 CCE-9123-1	PASS
3 - 79	網域成員：安全通道資料加以數位加密或簽章(自動) CCE-8974-8	PASS
3 - 80	網域成員：要求增強式 (Windows 2000 或更新) 工作階段金鑰 CCE-9387-2	PASS

3 - 81	網域成員：安全通道資料加以數位加密 (可能的話) CCE-9251-0	PASS
3 - 82	網域成員：安全通道資料加以數位簽章 (可能的話) CCE-9375-7	PASS
3 - 83	MSS : (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended , 5 is default) CCE-9487-0	PASS
3 - 84	MSS : (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) CCE-8655-3	PASS
3 - 85	MSS : (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) CCE-9456-5	PASS
3 - 86	MSS : (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) CCE-9458-1	PASS
3 - 87	MSS : (KeepAliveTime) How often keep-alive packets are sent in milliseconds CCE-9426-8	PASS
3 - 88	MSS : (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes CCE-8513-4	PASS
3 - 89	MSS : (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS) CCE-1967-9	PASS
3 - 90	MSS : (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) CCE-9496-1	PASS
3 - 91	MSS : (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers CCE-8562-1	PASS
3 - 92	MSS : (Hidden) Hide computer from the browse list (Not Recommended except for highly secure environments) CCE-8560-5	PASS
3 - 93	MSS : (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic CCE-9439-1	PASS
3 - 94	MSS : (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning CCE-9501-8	PASS
3 - 95	MSS : (SafeDllSearchMode) Enable Safe DLL search mode (recommended) CCE-9348-4	PASS
3 - 96	MSS : (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) CCE-8591-0	PASS
3 - 97	MSS : (AutoAdminLogon) Enable Automatic Logon (not recommended) CCE-1967-9	PASS
3 - 98	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 CCE-9301-3	PASS
3 - 99	取得檔案或其他物件的擁有權 CCE-9309-6	PASS
3 - 100	同步處理目錄服務資料 CCE-10251-7	PASS
3 - 101	關閉系統 CCE-9014-2	PASS
3 - 102	還原檔案及目錄 CCE-9124-9	PASS
3 - 103	取代處理程序等級權杖 CCE-8732-0	PASS
3 - 104	從銜接站移除電腦 CCE-8732-0	PASS
3 - 105	設定檔系統效能 CCE-9419-3	PASS
3 - 106	設定檔單一處理程序 CCE-9388-0	PASS
3 - 107	執行磁碟區維護工作 CCE-8475-6	PASS
3 - 108	修改軟體環境值 CCE-9417-7	PASS
3 - 109	修改物件標籤 CCE-9149-6	PASS
3 - 110	管理稽核及安全性記錄檔 CCE-9223-9	PASS
3 - 111	以服務方式登入 CCE-9461-5	PASS
3 - 112	以批次工作登入 CCE-9320-3	PASS
3 - 113	鎖定記憶體中的分頁 CCE-9289-0	PASS
3 - 114	載入及解除載入裝置驅動程式 CCE-9135-5	PASS
3 - 115	增加排程優先順序 CCE-8999-5	PASS
3 - 116	增加處理程序工作組 CCE-9048-0	PASS

3 - 117	在驗證後模擬用戶端 CCE-8467-3	PASS
3 - 118	產生安全性稽核 CCE-9226-2	PASS
3 - 119	強制從遠端系統進行關閉 CCE-9336-9	PASS
3 - 120	拒絕本機登入 CCE-9239-5	PASS
3 - 121	拒絕以服務方式登入 CCE-9098-5	PASS
3 - 122	拒絕以批次工作登入 CCE-9212-2	PASS
3 - 123	拒絕從網路存取這台電腦 CCE-9244-5	PASS
3 - 124	偵錯程式 CCE-8583-7	PASS
3 - 125	建立符號連結 CCE-8460-8	PASS
3 - 126	建立永久共用物件 CCE-9254-4	PASS
3 - 127	建立通用物件 CCE-8431-9	PASS
3 - 128	建立權杖物件 CCE-9215-5	PASS
3 - 129	建立分頁檔 CCE-9185-0	PASS
3 - 130	變更時區 CCE-8423-6	PASS
3 - 131	變更系統時間 CCE-8612-4	PASS
3 - 132	略過周遊檢查 CCE-8414-5	PASS
3 - 133	備份檔案及目錄 CCE-9389-8	PASS
3 - 134	允許本機登入 CCE-9345-0	PASS
3 - 135	調整處理程序的記憶體配額 CCE-9068-8	PASS
3 - 136	當成作業系統的一部分 CCE-9407-8	PASS
3 - 137	從網路存取這台電腦 CCE-9253-6	PASS
3 - 138	允許透過遠端桌面服務登入 CCE-9107-4	PASS
3 - 139	拒絕透過遠端桌面服務登入 CCE-9274-2	PASS
3 - 140	傳真 CCE-10150-1	PASS
3 - 141	提升權限時列舉系統管理員帳戶 CCE-9938-2	PASS
3 - 142	關閉網頁發布和線上訂購精靈的網際網路下載 CCE-9674-3	PASS
3 - 143	關閉網際網路檔案關聯服務 CCE-10795-3	PASS
3 - 144	關閉「訂購沖印」圖片工作 CCE-9823-6	PASS
3 - 145	關閉檔案及資料夾的「發布到網站」工作 CCE-9643-8	PASS
3 - 146	關閉事件檢視器 "Events.asp" 連結 CCE-9819-4	PASS
3 - 147	關閉 Windows Messenger 客戶經驗改進計劃 CCE-9559-6	FAIL
3 - 148	關閉 Windows 錯誤報告 CCE-10441-4	PASS
3 - 149	關閉搜尋小幫手內容檔更新 CCE-10140-2	PASS
3 - 150	關閉手寫辨識錯誤報告 CCE-10645-0	PASS
3 - 151	如果 URL 連線正在參照 Microsoft.com 時，關閉網際網路連線精靈 CCE-10649-2	PASS
3 - 152	如果 URL 連線正在參照 Microsoft.com 時，關閉註冊 CCE-10160-0	PASS

3 - 153	關閉個人化手寫資料共用 CCE-10658-3	PASS
3 - 154	關閉透過 HTTP 下載印表機驅動程式 CCE-9195-9	PASS
3 - 155	關閉 HTTP 上的列印 CCE-10061-0	PASS
3 - 156	不要處理只執行一次清單 CCE-10154-3	PASS
3 - 157	永遠使用傳統登入 CCE-10591-6	FAIL
3 - 158	關閉自動播放 CCE-9528-1	FAIL
3 - 159	AutoRun 的預設行為 CCE-10527-0	PASS
3 - 160	關閉非磁碟區裝置的自動播放 CCE-10655-9	PASS
3 - 161	關閉殼層通訊協定受保護模式 CCE-10623-7	PASS
3 - 162	損毀時關閉終止堆集 CCE-9874-9	PASS
3 - 163	關閉檔案總管的資料執行防止 CCE-9918-4	PASS
3 - 164	防止 Windows Anytime Upgrade 執行 CCE-10137-8	PASS
3 - 165	於使用者登入期間，報告登入伺服器無法使用 CCE-9907-7	PASS
3 - 166	限制解壓縮和安裝未經數位簽署的小工具 CCE-10811-8	PASS
3 - 167	關閉桌面小工具 CCE-10801-9	PASS
3 - 168	關閉使用者安裝的桌面小工具 CCE-10586-6	PASS
3 - 169	覆寫其他小工具連結 CCE-9857-4	FAIL
3 - 170	停用遠端桌面共用 CCE-10763-1	PASS
3 - 171	關閉自動下載隨函附件 CCE-10730-0	PASS
3 - 172	顯示錯誤通知 CCE-10709-4	FAIL
3 - 173	停用記錄 CCE-10157-6	PASS
3 - 174	不傳送其他資料 CCE-10824-1	PASS
3 - 175	關閉 Microsoft 對等網路服務 CCE-10438-0	PASS
3 - 176	喚醒電腦時必須使用密碼(使用電池) CCE-9829-3	PASS
3 - 177	喚醒電腦時必須使用密碼(一般電源) CCE-9670-1	PASS
3 - 178	設定 Windows NTP 用戶端 CCE-10500-7	PASS
3 - 179	關閉程式清查 CCE-10787-0	PASS
3 - 180	防止從網際網路擷取裝置中繼資料 CCE-10165-9	PASS
3 - 181	允許遠端存取隨插即用介面 CCE-10769-8	PASS
3 - 182	當裝置上已安裝標準驅動程式時，不要傳送 Windows 錯誤報告 CCE-9901-0	PASS
3 - 183	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 CCE-10553-6	PASS
3 - 184	指定搜尋裝置驅動程式的來源位置時的搜尋順序 CCE-9919-2	PASS
3 - 185	不允許執行數位購物服務區 CCE-10759-9	PASS
3 - 186	記錄檔大小上限 (KB)-應用程式 CCE-9603-2	PASS
3 - 187	關閉遊戲資訊下載 CCE-10828-2	FAIL
3 - 188	關閉遊戲更新 CCE-10850-6	FAIL

3 - 189	登錄原則處理 CCE-9361-7	PASS
3 - 190	防止電腦加入 HomeGroup CCE-10183-2	PASS
3 - 191	停用 Windows Installer 指令碼的 IE 安全性提示 CCE-9875-6	PASS
3 - 192	允許使用者控制安裝 CCE-9876-4	PASS
3 - 193	禁止非系統管理員套用於廠商簽署的更新 CCE-9888-9	PASS
3 - 194	開啟 Mapper I/O(LLTDIO) 驅動程式 CCE-9783-2	PASS
3 - 195	開啟 Responder(RSPNDR) 驅動程式 CCE-10059-4	PASS
3 - 196	禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接 CCE-9953-1	FAIL
3 - 197	要求網域使用者在設定網路的位置時必須提升權限 CCE-10359-8	PASS
3 - 198	透過內部網路路由傳送所有流量 CCE-10509-8	FAIL
3 - 199	Microsoft 支援服務診斷工具：開啟與支援提供者的 MSDT 互動式通訊 CCE-9842-6	PASS
3 - 200	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-WQTS) CCE-10606-2	PASS
3 - 201	6to4 狀態 CCE-10266-5	PASS
3 - 202	ISATAP 狀態 CCE-10130-3	PASS
3 - 203	Teredo 狀態 CCE-10011-5	PASS
3 - 204	IP-HTTPS 狀態 CCE-10764-9	PASS
3 - 205	使用 Windows Connect Now 進行無線設定 CCE-9879-8	PASS
3 - 206	禁止存取 Windows Connect Now 精靈 CCE-10778-9	PASS
3 - 207	啟用或停用 PrefTrack CCE-10219-4	PASS
3 - 208	允許加密檔案索引 CCE-10496-8	PASS
3 - 209	啟用為未快取之 Exchange 資料夾編製索引的功能 CCE-9866-5	FAIL
3 - 210	設定自動更新 CCE-9403-7	PASS
3 - 211	不要在「關閉 Windows」對話方塊中顯示「安裝更新並關機」選項 CCE-9464-9	PASS
3 - 212	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 CCE-9672-7	PASS
3 - 213	重新排程已經排程好的自動更新安裝 CCE-10205-3	PASS
3 - 214	關閉社群 CCE-11252-4	PASS
3 - 215	關閉 Windows Mail 應用程式 CCE-11252-4	PASS
3 - 216	擴充指向並列印連線以搜尋 Windows Update CCE-11252-4	PASS
3 - 217	未經驗證的 RPC 用戶端限制 CCE-9396-3	PASS
3 - 218	RPC 端點對應程式用戶端驗證 CCE-10181-6	PASS
3 - 219	提供遠端協助 CCE-9960-6	PASS
3 - 220	請求遠端協助 CCE-9506-7	PASS
3 - 221	開啟工作階段紀錄 CCE-10344-0	PASS
3 - 222	不允許儲存密碼 CCE-10090-9	PASS
3 - 223	允許使用者使用遠端桌面服務從遠端連線 CCE-9985-3	FAIL
3 - 224	連線時永遠提示密碼 CCE-10103-0	PASS

3 - 225	設定用戶端連線加密層級 CCE-9764-2	PASS
3 - 226	未使用中但閒置的遠端桌面服務工作階段設定時間限制 CCE-10608-8	PASS
3 - 227	設定已斷線工作階段的時間限制 CCE-9858-2	PASS
3 - 228	結束後不刪除暫存資料夾 CCE-10856-3	PASS
3 - 229	不要使用每一工作階段的暫存資料夾 CCE-9864-0	PASS
3 - 230	不要顯示「安裝第一次使用」對話方塊 CCE-10692-2	PASS
3 - 231	防止自動更新 CCE-10602-1	PASS
3 - 232	防止 Windows Media DRM 網路網路存取 CCE-9908-5	PASS
3 - 241	設定 Microsoft SpyNet 報告 CCE-9868-1	PASS
3 - 242	停用 Windows 錯誤報告 CCE-9914-3	PASS
3 - 243	關機：清除虛擬記憶體分頁檔 CCE-9222-1	PASS
3 - 244	記錄檔大小上限 (KB)-安全性 CCE-9967-1	PASS
3 - 245	記錄檔大小上限 (KB)-安裝程式 CCE-10714-4	PASS
3 - 246	記錄檔大小上限 (KB)-系統 CCE-10156-8	PASS

User Settings		PASS
4 - 233	不要保留檔案附件的區域資訊 CCE-10166-7	PASS
4 - 234	隱藏移除區域資訊的機制 CCE-9684-2	PASS
4 - 235	開啟附件時通知防毒程式 CCE-10076-8	PASS
4 - 236	防止使用者共用其設定檔內的檔案 CCE-10644-3	PASS
4 - 237	關閉說明分級 CCE-10295-4	PASS
4 - 238	啟用螢幕保護裝置 CCE-10051-1	PASS
4 - 239	以密碼保護螢幕保護裝置 CCE-9730-3	PASS
4 - 240	螢幕保護裝置逾時 CCE-10148-5	PASS

Firewall Settings		FAIL
5 - 1	Windows 防火牆：禁止通知 CCE-9774-1	PASS
5 - 2	Windows 防火牆：禁止單點傳送回應到多點傳送或廣播要求 CCE-9069-6	PASS
5 - 3	Windows 防火牆：保護所有網路連線 CCE-9465-6	PASS
5 - 4	網域設定檔：套用本機防火牆規則 CCE-9686-7	PASS
5 - 5	網域設定檔：套用本機連線安全性規則 CCE-9329-4	PASS
5 - 6	網域設定檔：輸出連線 CCE-9509-1	PASS
5 - 7	網域設定檔：輸入連線 CCE-9620-6	PASS
5 - 8	網域設定檔：記錄丟棄的封包 CCE-10502-3	PASS
5 - 9	網域設定檔：記錄成功的連線 CCE-10268-1	PASS
5 - 10	網域設定檔：大小限制 CCE-9747-7	PASS
5 - 11	網域設定檔：名稱 CCE-10022-2	PASS

5 - 12	私人設定檔：顯示通知 CCE-8884-9	PASS
5 - 13	私人設定檔：允許單點傳播回應 CCE-9522-4	PASS
5 - 14	私人設定檔：套用本機防火牆規則 CCE-9663-6	PASS
5 - 15	私人設定檔：套用本機連線安全性規則 CCE-9712-1	PASS
5 - 16	私人設定檔：防火牆狀態 CCE-9739-4	PASS
5 - 17	私人設定檔：輸出連線 CCE-8870-8	PASS
5 - 18	私人設定檔：輸入連線 CCE-9694-1	PASS
5 - 19	私人設定檔：名稱 CCE-10386-1	PASS
5 - 20	私人設定檔：大小限制 CCE-10250-9	PASS
5 - 21	私人設定檔：記錄丟棄的封包 CCE-10215-2	PASS
5 - 22	私人設定檔：記錄成功的連線 CCE-10611-2	PASS
5 - 23	公用設定檔：顯示通知 CCE-9742-8	PASS
5 - 24	公用設定檔：允許單點傳播回應 CCE-9773-3	PASS
5 - 25	公用設定檔：套用本機防火牆規則 CCE-9786-5	PASS
5 - 26	公用設定檔：套用本機連線安全性規則 CCE-9817-8	PASS
5 - 27	公用設定檔：防火牆狀態 CCE-9593-5	PASS
5 - 28	公用設定檔：輸出連線 CCE-9588-5	PASS
5 - 29	公用設定檔：輸入連線 CCE-9007-6	PASS
5 - 30	公用設定檔：大小限制 CCE-10373-9	PASS
5 - 31	公用設定檔：記錄丟棄的封包 CCE-9749-3	PASS
5 - 32	公用設定檔：記錄成功的連線 CCE-9753-5	PASS
5 - 33	公用設定檔：名稱 CCE-9926-7	PASS
5 - 34	核心網路功能-動態主機設定通訊協定 (DHCP-In) CCE-14986-4	FAIL
5 - 35	核心網路功能-IPv6 的動態主機設定通訊協定 (DHCPV6-In) CCE-14854-4	PASS

Internet Explorer		FAIL
6 - 1	Computer：包含來自 Microsoft 的更新網站清單 CCE-10603-9	FAIL
6 - 2	Computer：停用變更自動設定之設定 CCE-10638-5	FAIL
6 - 3	Computer：防止執行 [首次執行] 精靈 CCE-10641-9	FAIL
6 - 4	Computer：關閉 Internet Explorer 8 的管理 SmartScreen 的篩選工具 CCE-9973-9	PASS
6 - 5	Computer：不允許使用者啟用或停用附加元件 CCE-10235-0	FAIL
6 - 6	Computer：關閉當機偵測 CCE-10594-0	FAIL
6 - 7	Computer：關閉安全性設定檢查功能 CCE-10607-0	PASS
6 - 8	Computer：防止參與客戶經驗改進計畫 CCE-10522-1	FAIL
6 - 9	Computer：為每台電腦建立 Proxy 設定 - 而不是每個使用者 CCE-9870-7	PASS
6 - 10	Computer：安全性區域：不允許使用者新增與移除網站 CCE-10394-5	FAIL
6 - 11	Computer：安全性區域：不允許使用者變更原則 CCE-10037-0	FAIL

6 - 12	Computer : 安全區域 : 只使用電腦設定 CCE-10096-6	FAIL
6 - 13	Computer : 停用「設定記錄」 CCE-10387-9	FAIL
6 - 14	Computer : 允許結束時刪除瀏覽歷程紀錄 CCE-10590-8	PASS
6 - 15	Computer : 防止刪除使用者曾經造訪的網站 CCE-10110-5	PASS
6 - 16	Computer : 即使簽章無效也允許執行或安裝軟體 CCE-10052-9	PASS
6 - 17	Computer : 檢查所下載程式上的簽章 CCE-10055-2	FAIL
6 - 18	Computer : 允許其他廠商瀏覽器延伸 CCE-9905-1	FAIL
6 - 19	Computer : 自動檢查 Internet Explorer 更新 CCE-10581-7	PASS
6 - 20	Computer : 允許在使用者電腦上執行 CD 的主動式內容 CCE-10293-9	PASS
6 - 21	Computer : 檢查伺服器憑證撤銷 CCE-10074-3	FAIL
6 - 22	Computer : 關閉變更檢查 Internet Explorer 和網際網路工具更新時所顯示的 URL CCE-10595-7	FAIL
6 - 23	Computer : 關閉設定檢查更新的時間間隔(天) CCE-9776-6	FAIL
6 - 24	Computer : Internet Explorer 程序 - MK 通訊協定安全性限制 CCE-10265-7	FAIL
6 - 25	Computer : Internet Explorer 程序 - 一致的 MIME 處理 CCE-10138-6	FAIL
6 - 26	Computer : Internet Explorer 程序 - Mime 探查安全功能 CCE-10635-1	FAIL
6 - 27	Computer : Internet Explorer 程序 - 限制 ActiveX 安裝 CCE-10405-9	FAIL
6 - 28	Computer : Internet Explorer 程序 - 限制檔案下載 CCE-10578-3	FAIL
6 - 29	Computer : Internet Explorer 程序 - 已撰寫指令碼的 Windows 安全性限制 CCE-10604-7	FAIL
6 - 30	Computer : Internet Explorer 程序 - 來自區域高度的保護 CCE-10574-2	FAIL
6 - 31	Computer : 關閉「InPrivate 瀏覽」 CCE-9885-5	FAIL
6 - 32	Computer : JAVA 權限 - 鎖定的本機電腦區域 CCE-10535-3	FAIL
6 - 33	Computer : JAVA 權限 - 鎖定的內部網路區域 CCE-10342-4	FAIL
6 - 34	Computer : JAVA 權限 - 鎖定的信任的網站區域 CCE-10654-2	FAIL
6 - 35	Computer : 下載已簽署的 ActiveX 控制項 - 鎖定的網際網路區域 CCE-10095-8	FAIL
6 - 36	Computer : JAVA 權限 - 鎖定的網際網路區域 CCE-10597-3	FAIL
6 - 37	Computer : JAVA 權限 - 鎖定的受限制的網站區域 CCE-10275-6	FAIL
6 - 38	Computer : 內部網路網站 : 包含所有網路路徑 (UNC) CCE-9660-2	FAIL
6 - 39	Computer : JAVA 權限 - 本機電腦區域 CCE-10319-2	FAIL
6 - 40	Computer : JAVA 權限 - 內部網路區域 CCE-10566-8	FAIL
6 - 41	Computer : JAVA 權限 - 信任的網站區域 CCE-10566-8	FAIL
6 - 42	Computer : 自動提示檔案下載 - 網際網路區域 CCE-10566-8	FAIL
6 - 43	Computer : 下載未簽署的 ActiveX 控制項 - 網際網路區域 CCE-10433-1	FAIL
6 - 44	Computer : 下載已簽署的 ActiveX 控制項 - 網際網路區域 CCE-9917-6	FAIL
6 - 45	Computer : 起始不標示為安全的 ActiveX 控制項 - 網際網路區域 CCE-10561-9	FAIL
6 - 46	Computer : JAVA 權限 - 網際網路區域 CCE-10182-4	FAIL
6 - 47	Computer : 啟動在 IFRAME 中的應用程式及檔案 - 網際網路區域 CCE-9821-0	FAIL

6 - 48	Computer : 存取跨網域的資料來源 - 網際網路區域 CCE-10380-4	FAIL
6 - 49	Computer : 允許透過指令碼執行剪貼簿的剪下、複製或貼上作業 - 網際網路區域 CCE-10002-4	FAIL
6 - 50	Computer : 允許拖放或複製及貼上檔案 - 網際網路區域 CCE-10002-4	FAIL
6 - 51	Computer : 允許字型下載 - 網際網路區域 CCE-10403-4	FAIL
6 - 52	Computer : 允許安裝桌面項目 - 網際網路區域 CCE-9790-7	FAIL
6 - 53	Computer : 允許由指令碼起始沒有大小或位置限制的視窗 - 網際網路區域 CCE-9882-2	FAIL
6 - 54	Computer : 允許程式碼片段 - 網際網路區域 CCE-10685-6	FAIL
6 - 55	Computer : 允許透過指令碼進行更新狀態列 - 網際網路區域 CCE-9750-1	FAIL
6 - 56	Computer : 啟用 MIME 探查 - 網際網路區域 CCE-10107-1	FAIL
6 - 57	Computer : 軟體頻道權限 - 網際網路區域 CCE-10425-7	FAIL
6 - 58	Computer : 關閉第一次執行提示 - 網際網路區域 CCE-10434-9	FAIL
6 - 59	Computer : 開啟受保護模式 - 網際網路區域 CCE-10676-5	FAIL
6 - 60	Computer : 使用快顯封鎖程式 - 網際網路區域 CCE-10486-9	FAIL
6 - 61	Computer : 保留使用者資料 - 網際網路區域 CCE-10200-4	FAIL
6 - 62	Computer : 在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域 - 網際網路區域 CCE-10622-9	FAIL
6 - 63	Computer : 僅允許核准的網域使用 ActiveX 控制項而不提示 - 網際網路區域 CCE-9793-1	FAIL
6 - 64	Computer : 查閱不同網域內的視窗和框架 - 網際網路區域 CCE-9865-7	FAIL
6 - 65	Computer : 執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件 - 網際網路區域 CCE-10515-5	FAIL
6 - 66	Computer : 允許 Internet Explorer WebBrowser 控制項的指令碼 - 網際網路區域 CCE-9779-0	FAIL
6 - 67	Computer : 將檔案上傳到伺服器時包括本機路徑 - 網際網路區域 CCE-10646-8	FAIL
6 - 68	Computer : 顯示可能不安全檔案的安全警告 - 網際網路區域 CCE-10650-0	FAIL
6 - 69	Computer : 開啟跨網站指令碼篩選 - 網際網路區域 CCE-10276-4	FAIL
6 - 70	Computer : 允許載入 XAML 檔案 - 網際網路區域 CCE-10672-4	FAIL
6 - 71	Computer : 執行使用 Authenticode 簽署的 .NET Framework 相依元件 - 網際網路區域 CCE-10625-2	FAIL
6 - 72	Computer : 登入選項 - 網際網路區域 CCE-10472-9	FAIL
6 - 73	Computer : 存取跨網域的資料來源 - 受限制的網站區域 CCE-10525-4	FAIL
6 - 74	Computer : 允許使用中的指令碼處理 - 受限制的網站區域 CCE-10393-7	FAIL
6 - 75	Computer : 允許二進位和指令碼行為 - 受限制的網站區域 CCE-10547-8	FAIL
6 - 76	Computer : 允許透過指令碼執行剪貼簿的剪下、複製或貼上作業 - 受限制的網站區域 CCE-10539-5	FAIL
6 - 77	Computer : 允許拖放或複製及貼上檔案 - 受限制的網站區域 CCE-9667-7	FAIL
6 - 78	Computer : 允許檔案下載 - 受限制的網站區域 CCE-10466-1	FAIL
6 - 79	Computer : 允許字型下載 - 受限制的網站區域 CCE-9982-0	FAIL
6 - 80	Computer : 允許安裝桌面項目 - 受限制的網站區域 CCE-10475-2	FAIL
6 - 81	Computer : 允許 META REFRESH - 受限制的網站區域 CCE-10664-1	FAIL
6 - 82	Computer : 允許由指令碼起始沒有大小或位置限制的視窗 - 受限制的網站區域 CCE-9814-5	FAIL
6 - 83	Computer : 允許透過指令碼更新狀態列 - 受限制的網站區域 CCE-10431-5	FAIL

6 - 84	Computer : 自動提示檔案下載 - 受限制的網站區域 CCE-9959-8	FAIL
6 - 85	Computer : 下載已簽署的 ActiveX 控制項 - 受限制的網站區域 CCE-10470-3	FAIL
6 - 86	Computer : 下載未簽署的 ActiveX 控制項 - 受限制的網站區域 CCE-10461-2	FAIL
6 - 87	Computer : 起始不標示為安全的 ActiveX 控制項 - 受限制的網站區域 CCE-10347-3	FAIL
6 - 88	Computer : JAVA 權限 - 受限制的網站區域 CCE-10620-3	FAIL
6 - 89	Computer : 啟動在 IFRAME 中的應用程式及檔案 - 受限制的網站區域 CCE-10360-6	FAIL
6 - 90	Computer : 登入選項 - 受限制的網站區域 CCE-10651-8	FAIL
6 - 91	Computer : MIME 探查 - 受限制的網站區域 CCE-10277-2	FAIL
6 - 92	Computer : 執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件 - 受限制的網站區域 CCE-9898-8	FAIL
6 - 93	Computer : 執行使用 Authenticode 簽署的 .NET Framework 相依元件 - 受限制的網站區域 CCE-9673-5	FAIL
6 - 94	Computer : 執行 ActiveX 控制項及外掛程式 - 受限制的網站區域 CCE-9792-3	FAIL
6 - 95	Computer : 標示為安全的 ActiveX 控制項 - 受限制的網站區域 CCE-10554-4	FAIL
6 - 96	Computer : 以指令碼執行 Java Applet - 受限制的網站區域 CCE-10083-4	FAIL
6 - 97	Computer : 軟體頻道權限 - 受限制的網站區域 CCE-9669-3	FAIL
6 - 98	Computer : 關閉第一次執行提示 - 受限制的網站區域 CCE-10420-8	FAIL
6 - 99	Computer : 開啟受保護模式 - 受限制的網站區域 CCE-9945-7	FAIL
6 - 100	Computer : 使用快顯封鎖程式 - 受限制的網站區域 CCE-10094-1	FAIL
6 - 101	Computer : 保留使用者資料 - 受限制的網站區域 CCE-9760-0	FAIL
6 - 102	Computer : 在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域 - 受限制的網站區域 CCE-10609-6	FAIL
6 - 103	Computer : 僅允許核准的網域使用 ActiveX 控制項而不提示 - 受限制的網站區域 CCE-9832-7	FAIL
6 - 104	Computer : 查閱不同網域內的視窗和框架 - 受限制的網站區域 CCE-10642-7	FAIL
6 - 105	Computer : 允許 Internet Explorer WebBrowser 控制項的指令碼 - 受限制的網站區域 CCE-10725-0	FAIL
6 - 106	Computer : 將檔案上傳到伺服器時包括本機路徑 - 受限制的網站區域 CCE-9781-6	FAIL
6 - 107	Computer : 顯示可能不安全檔案的安全警告 - 受限制的網站區域 CCE-10744-1	FAIL
6 - 108	Computer : 開啟跨網站指令碼篩選 - 受限制的網站區域 CCE-10105-5	FAIL
6 - 109	Computer : 允許載入 XAML 檔案 - 受限制的網站區域 CCE-10178-2	FAIL
6 - 110	Computer : 允許程式碼片段 - 受限制的網站區域 CCE-10630-2	FAIL
6 - 111	User : 自動啟動 [網際網路連線精靈] CCE-15739-6	PASS
6 - 112	User : 停用表單自動完成功能 CCE-10388-7	PASS
6 - 113	User : 開啟表單上使用名稱和密碼的自動完成功能 CCE-10291-3	PASS
6 - 114	User : 停用 Internet Explorer 外部自訂 CCE-10829-0	PASS
6 - 115	User : 關閉畫面轉換 CCE-10701-1	PASS

規則技術細節

密碼必須符合複雜性需求

1. 打開 [控制台\系統管理工具\本機安全性原則\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求]
2. 啟用 (GCB 設定值為 啟用).

使用可還原的加密來存放密碼

1. 打開 [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]
2. 停用

關閉顯示器(使用電池)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定
3. 在右邊窗點擊 "關閉顯示器(使用電池)"
4. 輸入 "1200", 按 "確定"

關閉顯示器(使用一般電源)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 電腦設定\系統範本設定\系統\電源管理\視訊與顯示設定
3. 在右邊窗點擊 "關閉顯示器(使用一般電源)"
4. 輸入 "1200", 按 "確定"

指定系統休眠逾時(使用電池)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 電腦設定\系統範本設定\系統\電源管理\睡眠設定
3. 在右邊窗點擊 "指定系統休眠逾時(使用電池)"
4. 輸入 "3600", 按 "確定"

指定系統休眠逾時(使用一般電源)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 電腦設定\系統範本設定\系統\電源管理\睡眠設定
3. 在右邊窗點擊 "指定系統休眠逾時(使用一般電源)"
4. 輸入 "3600", 按 "確定"

網路安全性：強制限制登入時數

1. 打開 [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]
2. 啟用 (GCB 設定值為 啟用).

帳戶：重新命名系統管理員帳戶

建議重命名管理員帳戶.

1. 打開 [控制台\系統管理工具\本機安全性原則\安全性選項\帳戶：重新命名系統管理員帳戶]
2. 輸入新的管理員帳戶名稱. (GCB 設定值: Renamed_Admin)

帳戶：重新命名來賓帳戶名稱

建議重命名管理員帳戶.

1. 打開 [控制台\系統管理工具\本機安全性原則\安全性選項\帳戶：重新命名來賓帳戶名稱]
2. 輸入新的來賓帳戶名稱. (GCB 設定值: Renamed_Guest)

網路存取：允許匿名 SID_名稱轉譯

建議重命名管理員帳戶.

1. 打開 [控制台\系統管理工具\本機原則\安全性選項\網路存取：允許匿名SID/名稱轉譯]
2. 停用

帳戶：Administrator 帳戶狀態

建議重命名管理員帳戶.

1. 打開 [控制台\系統管理工具\本機原則\安全性選項\帳戶：Administrator 帳戶狀態]
2. 停用

帳戶：Guest 帳戶狀態

建議重命名管理員帳戶.

1. 打開 [控制台\系統管理工具\本機原則\安全性選項\帳戶：Guest 帳戶狀態]
2. 停用

修復主控台：允許自動系統管理登入

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "修復主控台：允許自動系統管理登入"
4. 選擇 "停用", 按 "確定".

修復主控台：允許軟體複製以及存取所有磁碟和所有資料夾

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "修復主控台：允許軟體複製以及存取所有磁碟和所有資料夾"
4. 選擇 "停用", 按 "確定".

裝置：CD-ROM 存取只限於登入本機的使用者

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "裝置：CD-ROM 存取只限於登入本機的使用者"
4. 選擇 "停用", 按 "確定".

裝置：軟碟機存取只限於登入本機的使用者

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "裝置：軟碟機存取只限於登入本機的使用者"
4. 選擇 "停用", 按 "確定".

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "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"
4. 輸入 "2", 按 "確定". (GCB 設定值為 2)

互動式登入：要求網域控制站驗證以解除鎖定工作站

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：要求網域控制站驗證以解除鎖定工作站"
4. 選擇 "停用", 按 "確定". (GCB 設定值為 停用)

互動式登入：在密碼到期前提示使用者變更密碼

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：在密碼到期前提示使用者變更密碼"
4. 輸入 "14", 按 "確定". (GCB 設定值為 14 天)

互動式登入：智慧卡移除操作

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：在密碼到期前提示使用者變更密碼"
4. 選擇 "鎖定工作站", 按 "確定". (GCB 設定值為 鎖定工作站)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "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"
4. 選擇 "提示要求同意", 按 "確定". (GCB 設定值為 提示要求同意)

使用者帳戶控制：標準使用者之提升權限提示的行為

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：標準使用者之提升權限提示的行為"
4. 選擇 "在安全桌面顯示輸入認證", 按 "確定". (GCB 設定值為 在安全桌面顯示輸入認證)

互動式登入：不要求按 CTRL+ALT+DEL 鍵

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：不要求按 CTRL+ALT+DEL 鍵"
4. 選擇 "停用", 按 "確定". (GCB 設定值為 停用)

互動式登入：不要顯示上次登入的使用者名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：不要顯示上次登入的使用者名稱"
4. 選擇 "啟用", 按 "確定"。(GCB 設定值為 啟用)

使用者帳戶控制：偵測應用程式安裝，並提示提升權限

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：偵測應用程式安裝，並提示提升權限"
4. 選擇 "啟用", 按 "確定"。(GCB 設定值為 啟用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "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"
4. 選擇 "啟用", 按 "確定"。(GCB 設定值為 啟用)

使用者帳戶控制：僅針對在安全位置安裝的 UIAccess 應用程式，提高其權限

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：僅針對在安全位置安裝的 UIAccess 應用程式，提高其權限"
4. 選擇 "啟用", 按 "確定"。(GCB 設定值為 啟用)

使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置", 按 "確定"。(GCB 設定值為 啟用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：使用內建的 Administrator 帳戶的管理員核准模式", 按 "啟用"。(GCB 設定值為 啟用)

網路安全性：設定 Kerberos 允許的加密類型

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路安全性：設定 Kerberos 允許的加密類型", 選擇 "RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, 未來的加密類型"。(GCB 設定值)

互動式登入：給登入使用者的訊息標題

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：給登入使用者的訊息標題", 輸入 "--WARNING--"。(GCB 設定值)

互動式登入：給登入使用者的訊息本文

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "互動式登入：給登入使用者的訊息本文", 輸入 "This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personal may provide the evidence of such monitoring to law enforcement officials."。(GCB 設定值)

使用者帳戶控制：提示提升權限時切換到安全桌面

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "使用者帳戶控制：提示提升權限時切換到安全桌面", 按 "啟用"。(GCB 設定值為 啟用)

關機：允許不登入就將系統關機

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "關機：允許不登入就將系統關機", 按 "啟用"。(GCB 設定值為 啟用)

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
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "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"，按 "停用"。(GCB 設定值為 停用)

稽核：稽核通用系統物件的存取
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "稽核：稽核通用系統物件的存取"，按 "停用"。(GCB 設定值為 停用)

網路存取：不允許存放網路驗證的密碼與認證
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路存取：不允許存放網路驗證的密碼與認證"，按 "啟用"。(GCB 設定值為 啟用)

網路存取：讓 Everyone 權限套用到匿名使用者
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路存取：讓 Everyone 權限套用到匿名使用者"，按 "停用"。(GCB 設定值為 停用)

系統加密編譯：Use FIPS 140 相容加密演算法，包括加密、雜湊以及簽署演算法
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "系統加密編譯：Use FIPS 140 相容加密演算法，包括加密、雜湊以及簽署演算法"，按 "啟用"。(GCB 設定值為 啟用)

網路存取：共用和安全性模式用於本機帳戶
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路存取：共用和安全性模式用於本機帳戶"，選擇 "傳統-本機使用者以自身身分驗證"。(GCB 設定值為 停用)

稽核：稽核備份與還原權限的使用
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "稽核：稽核備份與還原權限的使用"，按 "停用"。(GCB 設定值為 停用)

帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台"，按 "啟用"。(GCB 設定值為 啟用)

網路安全性：LAN Manager 驗證等級
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路安全性：LAN Manager 驗證等級"，選擇 "只傳送 NTLMv2 回應。拒絕 LM 和 NTLM"。(GCB 設定值)

網路安全性：允許 LocalSystem NULL 工作階段回復
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路安全性：允許 LocalSystem NULL 工作階段回復"，按 "停用"。(GCB 設定值為 停用)

網路安全性：NTLM SSP 為主的(包含安全 RPC)用戶端的最小工作階段安全性
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "網路安全性：NTLM SSP 為主的(包含安全 RPC)用戶端的最小工作階段安全性"，選擇 "要求NTLMv2工作階段安全性, 要求128位元加密"。(GCB 設定值)

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
<ol style="list-style-type: none"> 1. 執行 gpedit.msc 打開本機群組原則編輯器 2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 3. 在右邊窗點擊 "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"，選擇 "要求NTLMv2工作階段安全性, 要求128位元加密"。(GCB 設定值)

網路安全性：下次密碼變更時不儲存 LAN Manager 原則設定名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路安全性：下次密碼變更時不儲存 LAN Manager 原則設定名稱", 按 "啟用". (GCB 設定值為 啟用)

網路安全性：允許對此電腦的 PKU2U 驗證要求原則設定名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路安全性：允許對此電腦的 PKU2U 驗證要求原則設定名稱", 按 "停用". (GCB 設定值為 停用)

網路存取：不允許 SAM 帳戶和共用的匿名列舉

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：不允許 SAM 帳戶和共用的匿名列舉", 按 "啟用". (GCB 設定值為 啟用)

網路存取：不允許 SAM 帳戶的匿名列舉

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：不允許 SAM 帳戶的匿名列舉", 按 "啟用". (GCB 設定值為 啟用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "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以覆寫稽核原則類別設定", 按 "啟用". (GCB 設定值為 啟用)

網路安全性：允許 Local System 對 NTLM 使用電腦身分識別

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路安全性：允許 Local System 對 NTLM 使用電腦身分識別", 按 "啟用". (GCB 設定值為 啟用)

裝置：防止使用者安裝印表機驅動程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "裝置：防止使用者安裝印表機驅動程式", 按 "停用". (GCB 設定值為 停用)

網路存取：可遠端存取的登錄路徑

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：可遠端存取的登錄路徑", 輸入 "System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion".

網路存取：可遠端存取的登錄路徑及子路徑

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：可遠端存取的登錄路徑及子路徑", 輸入 "System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog".

系統物件：要求不區分大小寫用於非 Windows 子系統

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "系統物件：要求不區分大小寫用於非 Windows 子系統". (GCB 設定值為 啟用)

系統物件：加強內部系統物件的預設權限(例如：符號連結)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "系統物件：加強內部系統物件的預設權限(例如：符號連結)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間"
4. 輸入 "15"，按 "確定" (GCB 設定值為 15 分鐘)

網路伺服器：當登入時數到期時，中斷用戶端連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路伺服器：當登入時數到期時，中斷用戶端連線".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

網路存取：可以匿名存取的具名管道

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：可以匿名存取的具名管道"
4. 留下空白，按 "確定" (GCB 設定值為 空白)

網路存取：可以匿名存取的共用

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：可以匿名存取的共用"
4. 留下空白，按 "確定" (GCB 設定值為 空白)

Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

網路存取：限制匿名存取具名管道和共用

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：限制匿名存取具名管道和共用".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路存取：限制匿名存取具名管道和共用".
4. 選擇 "如果是用戶端所提供則接受"，點擊 "確定" (GCB 設定值為 如果是用戶端所提供則接受)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器"，按 "停用"。(GCB 設定值為 停用)

Microsoft 網路伺服器：數位簽章用戶端的通訊(如果伺服器同意)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路伺服器：數位簽章用戶端的通訊(如果伺服器同意)".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

網路安全性：LDAP用戶端簽章要求

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網路安全性：LDAP用戶端簽章要求".
4. 選擇 "交涉簽章", 點擊 "確定" (GCB 設定值為 交涉簽章)

網域成員：停用電腦帳戶密碼變更

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：停用電腦帳戶密碼變更", 按 "停用". (GCB 設定值為 停用)

網域成員：最長電腦帳戶密碼有效期

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：最長電腦帳戶密碼有效期", 輸入 "30". (GCB 設定值為 30 天)

網域成員：安全通道資料加以數位加密或簽章(自動)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：安全通道資料加以數位加密或簽章(自動)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

網域成員：要求增強式 (Windows 2000 或更新) 工作階段金鑰

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：要求增強式 (Windows 2000 或更新) 工作階段金鑰".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

網域成員：安全通道資料加以數位加密 (可能的話)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：安全通道資料加以數位加密 (可能的話)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

網域成員：安全通道資料加以數位簽章 (可能的話)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "網域成員：安全通道資料加以數位簽章 (可能的話)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

MSS : (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended , 5 is default)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)".
4. 選擇 "3", 點擊 "確定" (GCB 設定值為 3)

MSS : (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)".
4. 選擇 "Highest protection , source routing is completely disabled", 點擊 "確定" (GCB 設定值)

MSS : (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)".
4. 選擇 "3", 點擊 "確定" (GCB 設定值為 3)

MSS : (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

MSS : (KeepAliveTime) How often keep-alive packets are sent in milliseconds

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds".
4. 選擇 "300000 or 5 minutes(recommended)", 點擊 "確定" (GCB 設定值)

MSS : (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

MSS : (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

MSS : (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)".
4. 選擇 "Highest protection, source routing is completely disabled", 點擊 "確定" (GCB 設定值)

MSS : (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

MSS : (Hidden) Hide computer from the browse list (Not Recommended except for highly secure environments)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (Hidden) Hide computer from the browse list (Not Recommended except for highly secure environments)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

MSS : (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic".
4. 選擇 "Multicast, broadcast, and ISAKMP are exempt(Best for Windows XP)", 點擊 "確定" (GCB 設定值為 啟用)

MSS : (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning".
4. 選擇 "90", 點擊 "確定" (GCB 設定值)

MSS : (SafeDllSearchMode) Enable Safe DLL search mode (recommended)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

MSS : (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)".
4. 選擇 "5", 點擊 "確定" (GCB 設定值)

MSS : (AutoAdminLogon) Enable Automatic Logon (not recommended)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項
3. 在右邊窗點擊 "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"，按 "停用"。(GCB 設定值為 停用)

取得檔案或其他物件的擁有權

1. 打開 [電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\取得檔案或其他物件的擁有權]
2. 選擇 "Administrators"

同步處理目錄服務資料

關閉系統

1. 打開 [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]
2. 選擇 "Administrators, Users"

還原檔案及目錄

1. 打開 [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]
2. 選擇 "Administrators"

取代處理程序等級權杖

1. 打開 [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]
2. 選擇 "Local Service, Network Service"

從銜接站移除電腦

1. 打開 [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]
2. 選擇 "Administrators, Users"

設定檔系統效能

1. 打開 [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]
2. 選擇 "Administrators, WdiServiceHost"

設定檔單一處理程序

1. 打開 [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]
2. 選擇 "Administrators"

執行磁碟區維護工作

1. 打開 [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]
2. 選擇 "Administrators"

修改韌體環境值

1. 打開 [電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\修改韌體環境值]
2. 選擇 "Administrators"

修改物件標籤

1. 打開 [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]
2. 保留空白

管理稽核及安全性記錄檔

1. 打開 [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]
2. 選擇 "Administrators"

以服務方式登入

1. 打開 [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]
2. 保留空白

以批次工作登入

<p>1. 打開 [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]</p> <p>2. 保留空白</p>
<p>鎖定記憶體中的分頁</p> <p>1. 打開 [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]</p> <p>2. 保留空白</p>
<p>載入及解除載入裝置驅動程式</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Administrators"</p>
<p>增加排程優先順序</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Administrators"</p>
<p>增加處理程序工作組</p> <p>1. 打開 [電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\增加處理程序工作組]</p> <p>2. 選擇 "Administrators, Local Service"</p>
<p>在驗證後模擬用戶端</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Administrators, Local Service, Network Service, Service"</p>
<p>產生安全性稽核</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Local Service, Network Service"</p>
<p>強制從遠端系統進行關閉</p> <p>1. 打開 [電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\強制從遠端系統進行關閉]</p> <p>2. 選擇 "Administrators"</p>
<p>拒絕本機登入</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Guests"</p>
<p>拒絕以服務方式登入</p> <p>1. 執行 gpedit.msc 打開本機群組原則編輯器</p> <p>2. 選擇 [電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派]</p> <p>3. 在右邊窗點擊 "拒絕以服務方式登入"</p> <p>4. 保留空白, 按 "確定".</p>
<p>拒絕以批次工作登入</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Guests"</p>
<p>拒絕從網路存取這台電腦</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Guests"</p>
<p>偵錯程式</p> <p>1. 打開 [電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\強制從遠端系統進行關閉]</p> <p>2. 選擇 "Administrators"</p>
<p>建立符號連結</p> <p>1. 打開 [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]</p> <p>2. 選擇 "Administrators"</p>

<p>建立永久共用物件</p> <p>1. 打開 [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] 2. 保留空白</p>
<p>建立通用物件</p> <p>1. 打開 [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] 2. 選擇 "Administrators, Local Service, Network Service, Service"</p>
<p>建立權杖物件</p> <p>1. 打開 [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] 2. 保留空白</p>
<p>建立分頁檔</p> <p>1. 打開 [電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\建立分頁檔] 2. 選擇 "Administrators"</p>
<p>變更時區</p> <p>1. 打開 [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] 2. 選擇 "Administrators, Local Service, Users"</p>
<p>變更系統時間</p> <p>1. 打開 [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] 2. 選擇 "Administrators, Local Service"</p>
<p>略過周遊檢查</p> <p>1. 打開 [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] 2. 選擇 "Administrators, Local Service, Network Service, Users"</p>
<p>備份檔案及目錄</p> <p>1. 打開 [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] 2. 選擇 "Administrators"</p>
<p>允許本機登入</p> <p>1. 打開 [電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\允許本機登入] 2. 選擇 "Administrators, Users"</p>
<p>調整處理程序的記憶體配額</p> <p>1. 打開 [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] 2. 選擇 "Administrators, Local Service, Network Service"</p>
<p>當成作業系統的一部分</p> <p>1. 打開 [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] 2. 保留空白</p>
<p>從網路存取這台電腦</p> <p>1. 打開 [電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從網路存取這台電腦] 2. 選擇 "Administrators"</p>
<p>允許透過遠端桌面服務登入</p> <p>1. 打開 [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] 2. 選擇 "Remote Desktop Users, Administrators"</p>
<p>拒絕透過遠端桌面服務登入</p> <p>1. 打開 [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] 2. 選擇 "Guests"</p>

傳真

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows設定\安全性設定\系統服務]
3. 在右邊窗點擊 "Fax".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

提升權限時列舉系統管理員帳戶

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\認證使用者介面]
3. 在右邊窗點擊 "提升權限時列舉系統管理員帳戶".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

關閉網頁發布和線上訂購精靈的網際網路下載

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉網頁發布和線上訂購精靈的網際網路下載".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉網際網路檔案關聯服務

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉網際網路檔案關聯服務".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉「訂購沖印」圖片工作

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉「訂購沖印」圖片工作".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉檔案及資料夾的「發布到網站」工作

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉檔案及資料夾的「發布到網站」工作".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉事件檢視器 "Events.asp" 連結

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉事件檢視器 "Events.asp" 連結".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

關閉 Windows Messenger 客戶經驗改進計劃

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉 Windows Messenger 客戶經驗改進計劃".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉 Windows 錯誤報告

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉 Windows 錯誤報告".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉搜尋小幫手內容檔更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉搜尋小幫手內容檔更新".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉手寫辨識錯誤報告

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉手寫辨識錯誤報告".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

如果 URL 連線正在參照 Microsoft.com 時，關閉網際網路連線精靈

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "如果 URL 連線正在參照 Microsoft.com 時，關閉網際網路連線精靈".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

如果 URL 連線正在參照 Microsoft.com 時，關閉註冊

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "如果 URL 連線正在參照 Microsoft.com 時，關閉註冊".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉個人化手寫資料共用

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉個人化手寫資料共用".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉透過 HTTP 下載印表機驅動程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉透過 HTTP 下載印表機驅動程式".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉 HTTP 上的列印

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉 HTTP 上的列印".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

不要處理只執行一次清單

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\登入]
3. 在右邊窗點擊 "不要處理只執行一次清單".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

永遠使用傳統登入

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\登入]
3. 在右邊窗點擊 "永遠使用傳統登入".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉自動播放

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\自動播放原則]
3. 在右邊窗點擊 "關閉自動播放".
4. 選擇 "啟用"，選擇 "所有磁碟機"，點擊 "確定" (GCB 設定值為 啟用)

AutoRun 的預設行為

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\登入]
3. 在右邊窗點擊 "AutoRun 的預設行為".
4. 選擇 "啟用" 選擇 "不執行任何 Autorun 命令"，點擊 "確定" (GCB 設定值為 啟用)

關閉非磁碟區裝置的自動播放

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\自動播放原則]
3. 在右邊窗點擊 "關閉非磁碟區裝置的自動播放".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉殼層通訊協定受保護模式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 檔案總管]
3. 在右邊窗點擊 "關閉殼層通訊協定受保護模式".
4. 選擇 "停用"，點擊 "確定" (GCB 設定值為 停用)

損毀時關閉終止堆集

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 檔案總管]
3. 在右邊窗點擊 "損毀時關閉終止堆集".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

關閉檔案總管的資料執行防止

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 檔案總管]
3. 在右邊窗點擊 "關閉檔案總管的資料執行防止".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

防止 Windows Anytime Upgrade 執行

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Anytime Upgrade]
3. 在右邊窗點擊 "防止 Windows Anytime Upgrade 執行".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

於使用者登入期間, 報告登入伺服器無法使用

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 登入選項]
3. 在右邊窗點擊 "於使用者登入期間, 報告登入伺服器無法使用".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

限制解壓縮和安裝未經數位簽署的小工具

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\桌面小工具]
3. 在右邊窗點擊 "限制解壓縮和安裝未經數位簽署的小工具".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉桌面小工具

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\桌面小工具]
3. 在右邊窗點擊 "關閉桌面小工具".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉使用者安裝的桌面小工具

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\桌面小工具]
3. 在右邊窗點擊 "關閉使用者安裝的桌面小工具".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

覆寫其他小工具連結

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\桌面小工具]
3. 在右邊窗點擊 "覆寫其他小工具連結".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

停用遠端桌面共用

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\NetMeeting]
3. 在右邊窗點擊 "停用遠端桌面共用".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉自動下載隨函附件

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\RSS 摘要]
3. 在右邊窗點擊 "關閉自動下載隨函附件".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

顯示錯誤通知

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 錯誤報告]
3. 在右邊窗點擊 "顯示錯誤通知".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 啟用)

停用記錄

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 錯誤報告]
3. 在右邊窗點擊 "停用記錄".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

不傳送其他資料

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 錯誤報告]
3. 在右邊窗點擊 "不傳送其他資料".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉 Microsoft 對等網路服務

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\Microsoft 對等網路服務]
3. 在右邊窗點擊 "關閉 Microsoft 對等網路服務".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

喚醒電腦時必須使用密碼(使用電池)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\電源管理\睡眠設定]
3. 在右邊窗點擊 "喚醒電腦時必須使用密碼(使用電池)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

喚醒電腦時必須使用密碼(一般電源)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\電源管理\睡眠設定]
3. 在右邊窗點擊 "喚醒電腦時必須使用密碼(一般電源)".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

設定 Windows NTP 用戶端

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 時間服務\時間提供者]
3. 在右邊窗點擊 "設定 Windows NTP 用戶端".
4. 選擇 "啟用", 選擇 "NTP Server : time.nist.gov"
類型 : NT5DS
CrossSiteSyncFlags : 2
ResolvePeerBackoffMinutes : 15
ResolvePeerBackoffMaxTimes : 7
SpecialPollInterval : 3600
EventLogFlags : 0", 點擊 "確定" (GCB 設定值為 啟用)

關閉程式清查

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\應用程式相容性]
3. 在右邊窗點擊 "關閉程式清查".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

防止從網際網路擷取裝置中繼資料

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\裝置安裝]
3. 在右邊窗點擊 "防止從網際網路擷取裝置中繼資料".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

允許遠端存取隨插即用介面

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\裝置安裝]
3. 在右邊窗點擊 "允許遠端存取隨插即用介面"
4. 選擇 "已停用", 按 "確定"

當裝置上已安裝標準驅動程式時, 不要傳送 Windows 錯誤報告

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\裝置安裝]
3. 在右邊窗點擊 "當裝置上已安裝標準驅動程式時, 不要傳送 Windows 錯誤報告".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\裝置安裝]
3. 在右邊窗點擊 "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"
4. 選擇 "已停用"，按 "確定"

指定搜尋裝置驅動程式的來源位置時的搜尋順序

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\裝置安裝]
3. 在右邊窗點擊 "指定搜尋裝置驅動程式的來源位置時的搜尋順序".
4. 選擇 "啟用"，選擇 "不搜尋 Windows Update"，點擊 "確定" (GCB 設定值為 啟用)

不允許執行數位購物服務區

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\數位購物服務區]
3. 在右邊窗點擊 "不允許執行數位購物服務區".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

記錄檔大小上限 (KB)-應用程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\事件日誌服務\應用程式]
3. 在右邊窗點擊 "記錄檔大小上限 (KB)".
4. 選擇 "啟用" 輸入 32768 (KB)，點擊 "確定" (GCB 設定值為 啟用)

關閉遊戲資訊下載

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\遊戲總管]
3. 在右邊窗點擊 "關閉遊戲資訊下載".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

關閉遊戲更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\遊戲總管]
3. 在右邊窗點擊 "關閉遊戲更新".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

登錄原則處理

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\群組原則]
3. 在右邊窗點擊 "登錄原則處理".
4. 選擇 "啟用"，選擇 "即使群組原則物件尚未變更也進行處理"，點擊 "確定" (GCB 設定值為 啟用)

防止電腦加入 HomeGroup

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\HomeGroup]
3. 在右邊窗點擊 "防止電腦加入 HomeGroup".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 啟用)

停用 Windows Installer 指令碼的 IE 安全性提示

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Installer\]
3. 在右邊窗點擊 "停用 Windows Installer 指令碼的 IE 安全性提示".
4. 選擇 "停用"，點擊 "確定" (GCB 設定值為 停用)

允許使用者控制安裝

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Installer\]
3. 在右邊窗點擊 "允許使用者控制安裝".
4. 選擇 "停用"，點擊 "確定" (GCB 設定值為 停用)

禁止非系統管理員套用廠商簽署的更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Installer\]
3. 在右邊窗點擊 "禁止非系統管理員套用廠商簽署的更新".
4. 選擇 "啟用"，點擊 "確定" (GCB 設定值為 停用)

開啟 Mapper I/O(LLTDIO) 驅動程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\連結階層拓模搜尋]
3. 在右邊窗點擊 "開啟 Mapper I/O(LLTDIO) 驅動程式".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

開啟 Responder(RSPNDR) 驅動程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\連結階層拓模搜尋]
3. 在右邊窗點擊 "開啟 Responder(RSPNDR) 驅動程式".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\網路連線]
3. 在右邊窗點擊 "禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

要求網域使用者在設定網路的位置時必須提升權限

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\網路連線]
3. 在右邊窗點擊 "要求網域使用者在設定網路的位置時必須提升權限".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

透過內部網路路由傳送所有流量

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\網路連線]
3. 在右邊窗點擊 "透過內部網路路由傳送所有流量".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

Microsoft 支援服務診斷工具：開啟與支援提供者的 MSDT 互動式通訊

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "Microsoft 支援服務診斷工具：開啟與支援提供者的 MSDT 互動式通訊"
4. 選擇 "已停用", 按 "確定"

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)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\疑難排解與診斷\執行指令的診斷]
3. 在右邊窗點擊 "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)"
4. 選擇 "停用", 按 "確定"

6to4 狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\TCP設定值\IPv6 轉換技術]
3. 在右邊窗點擊 "6to4 狀態".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

ISATAP 狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術]
3. 在右邊窗點擊 "ISATAP 狀態".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

Teredo 狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術]
3. 在右邊窗點擊 "Teredo 狀態".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

IP-HTTPS 狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\TCP 設定值\IPv6 轉換技術]
3. 在右邊窗點擊 "IP-HTTPS 狀態".
4. 選擇 "啟用", 點擊 "確定", 在 "輸入IPHTTPS URL : " 輸入 "http://localhost", 選擇 "停用狀態" (GCB 設定值為 啟用)

使用 Windows Connect Now 進行無線設定

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\Windows Connect Now]
3. 在右邊窗點擊 "使用 Windows Connect Now 進行無線設定".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

禁止存取 Windows Connect Now 精靈

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\Windows Connect Now]
3. 在右邊窗點擊 "禁止存取 Windows Connect Now 精靈".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

啟用或停用 PrefTrack

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\疑難排解與診斷\Windows 效能 PrefTrack]
3. 在右邊窗點擊 "啟用/停用 PrefTrack".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

允許加密檔案索引

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\搜尋]
3. 在右邊窗點擊 "允許加密檔案索引".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

啟用為未快取之 Exchange 資料夾編製索引的功能

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\搜尋]
3. 在右邊窗點擊 "啟用為未快取之 Exchange 資料夾編製索引的功能".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

設定自動更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Update]
3. 在右邊窗點擊 "設定自動更新".
4. 選擇 "啟用", 選擇 "3-自動下載和通知我安裝", 點擊 "確定" (GCB 設定值為 啟用)

不要在「關閉 Windows」對話方塊中顯示「安裝更新並開機」選項

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Update]
3. 在右邊窗點擊 "不要在「關閉 Windows」對話方塊中顯示「安裝更新並開機」選項".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

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

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [系統管理範本\Windows 元件\Windows Update]
3. 在右邊窗點擊 "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".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

重新排程已經排程好的自動更新安裝

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Update]
3. 在右邊窗點擊 "重新排程已經排程好的自動更新安裝".
4. 選擇 "啟用", 選擇 1 分鐘, 點擊 "確定" (GCB 設定值為 啟用)

關閉社群

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Mail]
3. 在右邊窗點擊 "關閉社群".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉 Windows Mail 應用程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Mail]
3. 在右邊窗點擊 "關閉 Windows Mail 應用程式".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

擴充指向並列印連線以搜尋 Windows Update

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\印表機]
3. 在右邊窗點擊 "擴充指向並列印連線以搜尋 Windows Update".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

未經驗證的 RPC 用戶端限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\遠端程序呼叫]
3. 在右邊窗點擊 "未經驗證的 RPC 用戶端限制".
4. 選擇 "啟用", 選擇 "已驗證", 點擊 "確定" (GCB 設定值為 啟用)

RPC 端點對應程式用戶端驗證

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\遠端程序呼叫]
3. 在右邊窗點擊 "RPC 端點對應程式用戶端驗證".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

提供遠端協助

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\遠端協助]
3. 在右邊窗點擊 "提供遠端協助".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

請求遠端協助

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\遠端協助]
3. 在右邊窗點擊 "請求遠端協助".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

開啟工作階段紀錄

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\系統\遠端協助]
3. 在右邊窗點擊 "開啟工作階段紀錄".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

不允許儲存密碼

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "不允許儲存密碼".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

允許使用者使用遠端桌面服務從遠端連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "允許使用者使用遠端桌面服務從遠端連線".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

連線時永遠提示密碼

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "連線時永遠提示密碼".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

設定用戶端連線加密層級

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "設定用戶端連線加密層級".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

未使用中但閒置的遠端桌面服務工作階段設定時間限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "未使用中但閒置的遠端桌面服務工作階段設定時間限制".
4. 選擇 "啟用", 選擇 15 分鐘, 點擊 "確定" (GCB 設定值為 啟用)

設定已斷線工作階段的時間限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "設定已斷線工作階段的時間限制".
4. 選擇 "啟用", 選擇 15 分鐘, 點擊 "確定" (GCB 設定值為 啟用)

結束後不刪除暫存資料夾

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "結束後不刪除暫存資料夾".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

不要使用每一工作階段的暫存資料夾

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "不要使用每一工作階段的暫存資料夾".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

不要顯示「安裝第一次使用」對話方塊

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Media Player]
3. 在右邊窗點擊 "不要顯示「安裝第一次使用」對話方塊".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

防止自動更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Media Player]
3. 在右邊窗點擊 "防止自動更新".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

防止 Windows Media DRM 網路網路存取

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Media Digital Rights Management]
3. 在右邊窗點擊 "防止 Windows Media DRM 網路網路存取".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

設定 Microsoft SpyNet 報告

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows Defender]
3. 在右邊窗點擊 "設定 Microsoft SpyNet 報告".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

停用 Windows 錯誤報告

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Windows 錯誤報告]
3. 在右邊窗點擊 "停用 Windows 錯誤報告".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關機：清除虛擬記憶體分頁檔

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項]
3. 在右邊窗點擊 "關機：清除虛擬記憶體分頁檔", 按 "停用". (GCB 設定值為 停用)

記錄檔大小上限 (KB)-安全性

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\事件日誌服務\安全性]
3. 在右邊窗點擊 "記錄檔大小上限 (KB)".
4. 選擇 "啟用" 輸入 81920 (KB), 點擊 "確定" (GCB 設定值為 啟用)

記錄檔大小上限 (KB)-安裝程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\事件日誌服務\安裝程式]
3. 在右邊窗點擊 "記錄檔大小上限 (KB)".
4. 選擇 "啟用" 輸入 81920 (KB), 點擊 "確定" (GCB 設定值為 啟用)

記錄檔大小上限 (KB)-系統

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\事件日誌服務\系統]
3. 在右邊窗點擊 "記錄檔大小上限 (KB)".
4. 選擇 "啟用" 輸入 32768 (KB), 點擊 "確定" (GCB 設定值為 啟用)

不要保留檔案附件的區域資訊

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows 元件\附件管理員]
3. 在右邊窗點擊 "不要保留檔案附件的區域資訊".
4. 選擇 "停用", 點擊 "確定" (GCB 設定值為 停用)

隱藏移除區域資訊的機制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows 元件\附件管理員]
3. 在右邊窗點擊 "隱藏移除區域資訊的機制".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

開啟附件時通知防毒程式

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows 元件\附件管理員]
3. 在右邊窗點擊 "開啟附件時通知防毒程式".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

防止使用者共用其設定檔內的檔案

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows 元件\網路共用]
3. 在右邊窗點擊 "防止使用者共用其設定檔內的檔案".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

關閉說明分級

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 在右邊窗點擊 "關閉說明分級".
4. 選擇 "啟用", 點擊 "確定" (GCB 設定值為 啟用)

啟用螢幕保護裝置

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 使用者設定\系統管理範本\控制台
3. Windows 7: 選擇 [個人化]
Windows XP: 選擇 [顯示]
4. 選擇 "啟用螢幕保護裝置", 點擊 "已啟用"
5. 點擊 "確定".

以密碼保護螢幕保護裝置

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 使用者設定\系統管理範本\控制台
3. Windows 7: 選擇 [個人化]
Windows XP: 選擇 [顯示]
4. 點擊 "以密碼保護螢幕保護裝置", 點擊 "已啟用"
5. 點擊 "確定".

螢幕保護裝置逾時

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 使用者設定\系統管理範本\控制台
3. Windows 7: 選擇 [個人化]
Windows XP: 選擇 [顯示]
4. 點擊 "螢幕保護裝置逾時", 設定時間 900 秒
5. 點擊 "確定".

Windows 防火牆：禁止通知

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\網路\網路連線\Windows 防火牆\網路設定檔\]
3. 點擊 "Windows防火牆：禁止通知"
4. 選擇 "已停用"
5. 點擊 "確定".

Windows 防火牆：禁止單點傳送回應到多點傳送或廣播要求

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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\]
3. 點擊 "Windows 防火牆：禁止單點傳送回應到多點傳送或廣播要求"
4. 選擇 "已啟用"
5. 點擊 "確定".

Windows 防火牆：保護所有網路連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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\]
3. 點擊 "Windows 防火牆：保護所有網路連線"
4. 選擇 "已啟用"
5. 點擊 "確定".

網域設定檔：套用本機防火牆規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機防火牆規則"
4. 選擇 "否"
5. 點擊 "確定".

網域設定檔：套用本機連線安全性規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機連線安全性規則"
4. 選擇 "否"
5. 點擊 "確定".

網域設定檔：輸出連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸出連線"
4. 選擇 "允許(預設)"
5. 點擊 "確定".

網域設定檔：輸入連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸入連線"
4. 選擇 "封鎖(預設)"
5. 點擊 "確定".

網域設定檔：記錄丟棄的封包

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄丟棄的封包"
4. 選擇 "是"
5. 點擊 "確定".

網域設定檔：記錄成功的連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄成功的連線"
4. 選擇 "是"
5. 點擊 "確定".

網域設定檔：大小限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "大小限制"
4. 選擇 "16384"
5. 點擊 "確定".

網域設定檔：名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "名稱"
4. 輸入 "%windir%\system32\logfiles\firewall\domainfirewall.log"
5. 點擊 "確定".

私人設定檔：顯示通知

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\私人設定檔\自訂\防火牆設定]
3. 點擊 "顯示通知"
4. 選擇 "是"
5. 點擊 "確定".

私人設定檔：允許單點傳播回應

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\私人設定檔\自訂\防火牆設定]
3. 點擊 "允許單點傳播回應"
4. 選擇 "否"
5. 點擊 "確定".

私人設定檔：套用本機防火牆規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機防火牆規則"
4. 選擇 "否"
5. 點擊 "確定".

私人設定檔：套用本機連線安全性規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機連線安全性規則"
4. 選擇 "否"
5. 點擊 "確定".

私人設定檔：防火牆狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "防火牆狀態"
4. 選擇 "開啟 (建議選項)"
5. 點擊 "確定".

私人設定檔：輸出連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸出連線"
4. 選擇 "允許 (預設)"
5. 點擊 "確定".

私人設定檔：輸入連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸入連線"
4. 選擇 "封鎖 (預設)"
5. 點擊 "確定".

私人設定檔：名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸入連線"
4. 輸入 "%windir%\System32\LogFiles\Firewall\privatefirewall.log"
5. 點擊 "確定".

私人設定檔：大小限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "大小限制"
4. 選擇 "16384"
5. 點擊 "確定".

私人設定檔：記錄丟棄的封包

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄丟棄的封包"
4. 選擇 "是"
5. 點擊 "確定".

私人設定檔：記錄成功的連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄成功的連線"
4. 選擇 "是"
5. 點擊 "確定".

公用設定檔：顯示通知

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\公用設定檔\自訂\防火牆設定]
3. 點擊 "顯示通知"
4. 選擇 "是"
5. 點擊 "確定".

公用設定檔：允許單點傳播回應

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\內容\公用設定檔\自訂\防火牆設定]
3. 點擊 "允許單點傳播回應"
4. 選擇 "否"
5. 點擊 "確定".

公用設定檔：套用本機防火牆規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機防火牆規則"
4. 選擇 "否"
5. 點擊 "確定".

公用設定檔：套用本機連線安全性規則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "套用本機連線安全性規則"
4. 選擇 "否"
5. 點擊 "確定".

公用設定檔：防火牆狀態

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "防火牆狀態"
4. 選擇 "開啟 (建議選項)"
5. 點擊 "確定".

公用設定檔：輸出連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸出連線"
4. 選擇 "允許 (預設)"
5. 點擊 "確定".

公用設定檔：輸入連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸入連線"
4. 選擇 "封鎖 (預設)"
5. 點擊 "確定".

公用設定檔：大小限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "大小限制"
4. 選擇 "16384"
5. 點擊 "確定".

公用設定檔：記錄丟棄的封包

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄丟棄的封包"
4. 選擇 "是"
5. 點擊 "確定".

公用設定檔：記錄成功的連線

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "記錄成功的連線"
4. 選擇 "是"
5. 點擊 "確定".

公用設定檔：名稱

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [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]
3. 點擊 "輸入連線"
4. 輸入 "%windir%\system32\logfiles\firewall\publicfirewall.log"
5. 點擊 "確定".

核心網路功能-動態主機設定通訊協定 (DHCP-In)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\輸入規則]
3. 點擊 "輸入連線"
4. 啟用 "核心網路功能-動態主機設定通訊協定 (DHCP-In)"
5. 點擊 "確定".

核心網路功能-IPv6 的動態主機設定通訊協定 (DHCPV6-In)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\輸入規則]
3. 點擊 "輸入連線"
4. 啟用 "核心網路功能-IPv6 的動態主機設定通訊協定 (DHCPV6-In)"
5. 點擊 "確定".

Computer：包含來自 Microsoft 的更新網站清單

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Internet Explorer\相容性檢視]
3. 點擊 "包含來自 Microsoft 的更新網站清單"
4. 選擇 "停用"
5. 點擊 "確定".

Computer：停用變更自動設定之設定

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Internet Explorer]
3. 點擊 "停用變更自動設定之設定"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer：防止執行 [首次執行] 精靈

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Internet Explorer]
3. 點擊 "防止執行 [首次執行] 精靈"
4. 選擇 "啟用", 選擇 "直接到首頁"
5. 點擊 "確定".

Computer：關閉 Internet Explorer 8 的管理 SmartScreen 的篩選工具

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows 元件\Internet Explorer]
3. 點擊 "關閉 Internet Explorer 8 的管理 SmartScreen 的篩選工具"
4. 選擇 "啟用", 選擇 "關閉"
5. 點擊 "確定".

Computer : 不允許使用者啟用或停用附加元件

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "不允許使用者啟用或停用附加元件"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 關閉當機偵測

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "關閉當機偵測"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 關閉安全性設定檢查功能

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "關閉安全性設定檢查功能"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 防止參與客戶經驗改進計畫

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "防止參與客戶經驗改進計畫"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 為每台電腦建立 Proxy 設定 - 而不是每個使用者

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "為每台電腦建立 Proxy 設定 - 而不是每個使用者"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 安全性區域 : 不允許使用者新增與移除網站

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "安全性區域 : 不允許使用者新增/移除網站"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 安全性區域 : 不允許使用者變更原則

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "安全性區域 : 不允許使用者變更原則"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 安全區域 : 只使用電腦設定

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "安全區域 : 只使用電腦設定"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 停用「設定記錄」

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\刪除瀏覽歷程記錄]
3. 點擊 "停用「設定記錄」"
4. 選擇 "啟用", 選擇 "40" 天
5. 點擊 "確定".

Computer : 允許結束時刪除瀏覽歷程紀錄

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\刪除瀏覽歷程記錄]
3. 點擊 "允許結束時刪除瀏覽歷程紀錄"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 防止刪除使用者曾經造訪的網站

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\刪除瀏覽歷程記錄]
3. 點擊 "防止刪除使用者曾經造訪的網站"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 即使簽章無效也允許執行或安裝軟體

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "即使簽章無效也允許執行或安裝軟體"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 檢查所下載程式上的簽章

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "檢查所下載程式上的簽章"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 允許其他廠商瀏覽器延伸

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "允許其他廠商瀏覽器延伸"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 自動檢查 Internet Explorer 更新

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "自動檢查 Internet Explorer 更新"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 允許在使用者電腦上執行 CD 的主動式內容

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "允許在使用者電腦上執行 CD 的主動式內容"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : 檢查伺服器憑證撤銷

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\進階畫面]
3. 點擊 "檢查伺服器憑證撤銷"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 關閉變更檢查 Internet Explorer 和網際網路工具更新時所顯示的 URL

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路設定\元件更新\定期檢查\Internet Explorer 和網際網路工具更新]
3. 點擊 "防止變更檢查 Internet Explorer 和網際網路工具更新的 URL"
4. 選擇 "啟用", 選擇 "空白"
5. 點擊 "確定".

Computer : 關閉設定檢查更新的時間間隔 (天)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路設定\元件更新\定期檢查]
3. 點擊 "關閉設定檢查更新的時間間隔 (天)"
4. 選擇 "啟用", 選擇 "30 天"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - MK 通訊協定安全性限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\MK 通訊協定安全性限制]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - 一致的 MIME 處理

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\一致的 MIME 處理]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - Mime 探查安全功能

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\Mime 探查安全功能]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - 限制 ActiveX 安裝

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\限制 ActiveX 安裝]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - 限制檔案下載

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\限制檔案下載]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - 已撰寫指令碼的 Windows 安全性限制

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\已撰寫指令碼的 Windows 安全性限制]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : Internet Explorer 程序 - 來自區域高度的保護

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\安全性功能\來自區域高度的保護]
3. 點擊 "Internet Explorer 程序"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : 關閉「InPrivate 瀏覽」

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\隱私權]
3. 點擊 "關閉「InPrivate 瀏覽」"
4. 選擇 "啟用"
5. 點擊 "確定".

Computer : JAVA 權限 - 鎖定的本機電腦區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的信任的網站區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : JAVA 權限 - 鎖定的內部網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的內部網路區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : JAVA 權限 - 鎖定的信任的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的信任的網站區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : 下載已簽署的 ActiveX 控制項 - 鎖定的網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的網際網路區域]
3. 點擊 "下載已簽署的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "下載已簽署的 ActiveX 控制項: 停用"
5. 點擊 "確定".

Computer : JAVA 權限 - 鎖定的網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的網際網路區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : JAVA 權限 - 鎖定的受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\鎖定的受限制的網站區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : 內部網路網站 : 包含所有網路路徑 (UNC)

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面]
3. 點擊 "內部網路網站: 包含所有網路路徑 (UNC)"
4. 選擇 "停用"
5. 點擊 "確定".

Computer : JAVA 權限 - 本機電腦區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\本機電腦區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 停用JAVA"
5. 點擊 "確定".

Computer : JAVA 權限 - 內部網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\內部網路區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 高安全性"
5. 點擊 "確定".

Computer : JAVA 權限 - 信任的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\信任的網站區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限: 高安全性"
5. 點擊 "確定".

Computer : 自動提示檔案下載 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "自動提示檔案下載"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 下載未簽署的 ActiveX 控制項 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "下載未簽署的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 下載已簽署的 ActiveX 控制項 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "下載已簽署的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 起始不標示為安全的 ActiveX 控制項 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "起始不標示為安全的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : JAVA 權限 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "JAVA 權限 : 停用 JAVA"
5. 點擊 "確定".

Computer : 啟動在 IFRAME 中的應用程式及檔案 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "啟動在 IFRAME 中的應用程式及檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 存取跨網域的資料來源 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "存取跨網域的資料來源"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許透過指令碼執行剪貼簿的剪下、複製或貼上作業 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許透過指令碼執行剪貼簿的剪下、複製或貼上作業"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許拖放或複製及貼上檔案 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許拖放或複製及貼上檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許字型下載 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許字型下載"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許安裝桌面項目 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許安裝桌面項目"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許由指令碼起始沒有大小或位置限制的視窗 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許由指令碼起始沒有大小或位置限制的視窗"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許程式碼片段 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許程式碼片段"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許透過指令碼進行更新狀態列 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許透過指令碼進行更新狀態列"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 啟用 MIME 探查 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "啟用 MIME 探查"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 軟體頻道權限 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "軟體頻道權限"
4. 選擇 "啟用", 選擇 "高安全性"
5. 點擊 "確定".

Computer : 關閉第一次執行提示 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "關閉第一次執行提示"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 開啟受保護模式 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "開啟受保護模式"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 使用快顯封鎖程式 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "使用快顯封鎖程式"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 保留使用者資料 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "保留使用者資料"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 僅允許核准的網域使用 ActiveX 控制項而不提示 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "僅允許核准的網域使用 ActiveX 控制項而不提示"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 查閱不同網域內的視窗和框架 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "查閱不同網域內的視窗和框架"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許 Internet Explorer WebBrowser 控制項的指令碼 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許 Internet Explorer WebBrowser 控制項的指令碼"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 將檔案上傳到伺服器時包括本機路徑 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "將檔案上傳到伺服器時包括本機路徑"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 顯示可能不安全檔案的安全警告 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "顯示可能不安全檔案的安全警告"
4. 選擇 "啟用" 以及 "提示"
5. 點擊 "確定".

Computer : 開啟跨網站指令碼篩選 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "開啟跨網站指令碼篩選"
4. 選擇 "啟用" 以及 "啟用"
5. 點擊 "確定".

Computer : 允許載入 XAML 檔案 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "允許載入 XAML 檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 執行使用 Authenticode 簽署的 .NET Framework 相依元件 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "執行使用 Authenticode 簽署的 .NET Framework 相依元件"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 登入選項 - 網際網路區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\網際網路區域]
3. 點擊 "登入選項"
4. 選擇 "啟用" 以及 "提示"
5. 點擊 "確定".

Computer : 存取跨網域的資料來源 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "存取跨網域的資料來源"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許使用中的指令碼處理 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許使用中的指令碼處理"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許二進位和指令碼行為 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許二進位和指令碼行為"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許透過指令碼執行剪貼簿的剪下、複製或貼上作業 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許透過指令碼執行剪貼簿的剪下、複製或貼上作業"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許拖放或複製及貼上檔案 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許拖放或複製及貼上檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許檔案下載 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許檔案下載"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許字型下載 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許字型下載"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許安裝桌面項目 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許安裝桌面項目"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許 META REFRESH - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許 META REFRESH"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許由指令碼起始沒有大小或位置限制的視窗 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許由指令碼起始沒有大小或位置限制的視窗"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許透過指令碼更新狀態列 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許透過指令碼更新狀態列"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 自動提示檔案下載 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "自動提示檔案下載"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 下載已簽署的 ActiveX 控制項 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "下載已簽署的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 下載未簽署的 ActiveX 控制項 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "下載未簽署的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 起始不標示為安全的 ActiveX 控制項 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "起始不標示為安全的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : JAVA 權限 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "JAVA 權限"
4. 選擇 "啟用", 選擇 "停用 JAVA"
5. 點擊 "確定".

Computer : 啟動在 IFRAME 中的應用程式及檔案 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "啟動在 IFRAME 中的應用程式及檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 登入選項 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "登入選項"
4. 選擇 "啟用", 選擇 "匿名登入"
5. 點擊 "確定".

Computer : MIME 探查 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "MIME 探查"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 執行使用 Authenticode 簽署的 .NET Framework 相依元件 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "執行使用 Authenticode 簽署的 .NET Framework 相依元件"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 執行 ActiveX 控制項及外掛程式 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "執行 ActiveX 控制項及外掛程式"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 標示為安全的 ActiveX 控制項 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "標示為安全的 ActiveX 控制項"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 以指令碼執行 Java Applet - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "以指令碼執行 Java Applet"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 軟體頻道權限 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "軟體頻道權限"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 關閉第一次執行提示 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "關閉第一次執行提示"
4. 選擇 "啟用", 選擇 "啟用", "啟用"
5. 點擊 "確定".

Computer : 開啟受保護模式 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "開啟受保護模式"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 使用快顯封鎖程式 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "使用快顯封鎖程式"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 保留使用者資料 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "保留使用者資料"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 僅允許核准的網域使用 ActiveX 控制項而不提示 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "僅允許核准的網域使用 ActiveX 控制項而不提示"
4. 選擇 "啟用", 選擇 "啟用"
5. 點擊 "確定".

Computer : 查閱不同網域內的視窗和框架 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "查閱不同網域內的視窗和框架"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許 Internet Explorer WebBrowser 控制項的指令碼 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許 Internet Explorer WebBrowser 控制項的指令碼"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 將檔案上傳到伺服器時包括本機路徑 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "將檔案上傳到伺服器時包括本機路徑"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 顯示可能不安全檔案的安全警告 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "顯示可能不安全檔案的安全警告"
4. 選擇 "啟用" 以及 "停用"
5. 點擊 "確定".

Computer : 開啟跨網站指令碼篩選 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "開啟跨網站指令碼篩選"
4. 選擇 "啟用" 以及 "啟用"
5. 點擊 "確定".

Computer : 允許載入 XAML 檔案 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許載入 XAML 檔案"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

Computer : 允許程式碼片段 - 受限制的網站區域

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [電腦設定\系統管理範本\Windows元件\Internet Explorer\網際網路控制台\安全性畫面\受限制的網站區域]
3. 點擊 "允許程式碼片段"
4. 選擇 "啟用", 選擇 "停用"
5. 點擊 "確定".

User : 自動啟動 [網際網路連線精靈]

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows元件\Internet Explorer\網際網路設定\進階設定\網際網路連線精靈設定]
3. 點擊 "自動啟動 [網際網路連線精靈]"
4. 選擇 "停用"
5. 點擊 "確定".

User : 停用表單自動完成功能

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "停用表單自動完成功能"
4. 選擇 "啟用"
5. 點擊 "確定".

User : 開啟表單上使用名稱和密碼的自動完成功能

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "開啟表單上使用名稱和密碼的自動完成功能"
4. 選擇 "停用"
5. 點擊 "確定".

User : 停用 Internet Explorer 外部自訂

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows元件\Internet Explorer]
3. 點擊 "停用 Internet Explorer 外部自訂"
4. 選擇 "啟用"
5. 點擊 "確定".

User : 關閉畫面轉換

1. 執行 gpedit.msc 打開本機群組原則編輯器
2. 選擇 [使用者設定\系統管理範本\Windows元件\Internet Explorer\網際網路設定\進階設定\瀏覽]
3. 點擊 "關閉畫面轉換"
4. 選擇 "啟用"
5. 點擊 "確定".