

SMR GCB組態檢測模組

政府組態基準(Government Configuration Baseline, 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。

政府組態基準



政府組態基準係針對行政院及所屬機關之電腦系統環境，部署 Windows 7、Windows 8.1與 Windows Server 2008 R2以及Internet Explorer 8與Internet Explorer 11之一致性安全設定，其中包含下表內容，共計有 1,208 項設定項目。

| 項次 | 類別 | 項目名稱 | 項數 | 小計 |
|----|--------------------|---|-----|-----|
| 1 | Windows 7 | USGCB Account Policy | 9 | 240 |
| | | USGCB Windows 7 Computer Energy Policy | 4 | |
| | | USGCB Windows 7 Computer Settings | 219 | |
| | | USGCB Windows 7 User Settings | 8 | |
| 2 | Windows 7 Firewall | USGCB Windows 7 Firewall Settings | 33 | 33 |
| 3 | Internet | USGCB Internet Explorer 8 Computer Settings | 110 | 115 |
| | | USGCB Internet Explorer 8 User Settings | 5 | |
| 合計 | | | | 388 |



✓ 共388項

GCB偵測

透過本模組，可以檢視每台電腦套用情況按機關和部門查詢各組織對政府組態GCB的，套用結果另提供專業的報表格式內容。

| GPO | 描述 | 行政局設定值 | 目前設定值 | 比較結果 | 設定說明 | 備註 |
|-----------------------------|------------------------------|-------------|---------|------|----------------------|-----------------|
| Windows 7 Computer Settings | 關閉安全中心：允許對出電腦的防火牆設定更改或線上身份識別 | 禁用 | NONE | 不符合 | 禁用 | |
| Windows 7 Computer Settings | 懸掛：確保通用系統物件的命名 | 禁用 | 0 | 符合 | 禁用 | |
| Windows 7 Computer Settings | 互動式登入：不要顯示上次登入的密碼提示 | 啟用 | 0 | 不符合 | 登入畫面不會顯示上次登入的人的用戶名密碼 | |
| Windows 7 Computer Settings | 互動式登入：不要禁用 CTRL+ALT+DEL | 禁用 | ENABLED | 不符合 | 禁用 | |
| Windows 7 Computer Settings | 使用非網際網路：使用非網際網路時，不要顯示安全警告 | 啟用 | 1 | 符合 | 啟用 | |
| Windows 7 Computer Settings | 使用非網際網路：從搜尋和程式安裝，並顯示簡介欄位 | 啟用 | 1 | 符合 | 啟用 | |
| Windows 7 Computer Settings | 使用非網際網路：從搜尋和程式安裝，並顯示簡介欄位 | 在安全桌面顯示輸入認證 | 3 | 不符合 | 在安全桌面顯示輸入認證 | |
| Windows 7 Computer Settings | 互動式登入：不要將防病毒引擎停用或禁用 | 禁用 | ENABLED | 不符合 | 禁用 | 禁用防病毒引擎將使系統易受攻擊 |
| Windows 7 Computer Settings | 設置：已安裝的防病毒引擎是否應自動更新 | 禁用 | ENABLED | 不符合 | 禁用 | |
| Windows 7 Computer Settings | 使用非網際網路：從搜尋和程式安裝，並顯示簡介欄位 | 顯示安全警告 | 0 | 不符合 | 顯示安全警告 | |

| GPO | 描述 | 行政局設定值 | 目前設定值 | 比較結果 | 設定說明 | 備註 |
|---------------------------------------|---------------------------------|--------|-------|------|---|----|
| Internet Explorer 8 | 檢查已下載網頁的檔案 | 啟用 | NONE | 不符合 | 啟用 | |
| Internet Explorer 8 Computer | 允許使用中的命令碼處理 | 啟用/禁用 | NONE | 符合 | 禁止執行區域中網頁的命令碼 | |
| Internet Explorer 8 Computer | 含有網際網路的資料來源 | 啟用/禁用 | NONE | 符合 | 從含有網際網路的資料來源下載內容，包括在瀏覽器內來自另一種語言的資料 | |
| Internet Explorer 8 Computer | 執行沒有使用 Authenticode 簽署 | 啟用/禁用 | NONE | 符合 | Internet Explorer 將不會對「未經簽署的網頁」區域，執行其重要的交際層元件 | |
| Internet Explorer 8 Computer Settings | 阻止對檔案的網際網路 ActiveX 控制項的執行 | 啟用/禁用 | NONE | 符合 | 阻止 ActiveX 控制項在區域中的網頁上執行。此設定將不會影響到：此項設定不會影響 ActiveX 控制項在下列區域中的網頁上執行 | |
| Internet Explorer 8 Computer Settings | 金鑰字元網際網路的預設初始值 | 啟用/禁用 | NONE | 符合 | 從安全桌面及其相關功能對搜尋和程式安裝的預設初始值 | |
| Internet Explorer 8 Computer Settings | Internet Explorer 網際網路安全警告的顯示時機 | 啟用/禁用 | NONE | 符合 | 決定顯示安全警告 | |
| Internet Explorer 8 Computer Settings | 使用防病毒引擎 | 啟用/禁用 | NONE | 符合 | 對「已安裝的防病毒引擎」狀態顯示人的狀態 | |
| Internet Explorer 8 Computer Settings | 金鑰字元網際網路 | 啟用/禁用 | NONE | 符合 | 決定顯示安全警告 | |
| Internet Explorer 8 Computer Settings | 阻止少時時延的網頁內容 | 啟用/禁用 | NONE | 符合 | 防止可能延遲的網頁內容，防止延遲的網頁內容，防止延遲的網頁內容 | |
| Internet Explorer 8 Computer Settings | 將電腦上與網際網路的連接，從本地網際網路 | 啟用/禁用 | NONE | 符合 | 決定顯示安全警告 | |