WinMatrix IT 資源管理系統 3.9.x 版 GCB 稽核模組功能規格表

GCB(政府組態基準)稽核模組 (此為選購功能)		
GCB 稽核	功能效益	
	・ 主動稽核電腦系統的安全性設定，是否落實政府組態基準 (Government Configuration Baseline，簡稱 GCB)規範的設定，以利先期發現盡早改善，確保機關中的電腦有一定程度的資安治理，增進作業環境的資訊安全。 ・ 機關權責人員可透過 Web 畫面的圖表，清楚知道合規與不合規的比例，並定期通報給管理人員，簡化管理檢視的複雜度，大幅提升可落實的程度，並降低作業負擔。	
	編號	功能項目
	1-1	自動收集端末電腦的安全性原則設定，項目包含： (1) 帳戶安全性：對於密碼原則、密碼長度、帳戶鎖定原則等組態進行檢測 (2) 電腦設定：檢測安全性選項、使用者權限指派、網際網路通訊設定、自動播放等組態 (3) 使用者設定：檢測螢幕保護裝置、網際網路通訊、網路共用、附件管理員等組態 (4) 瀏覽器組態: 檢測 IE、Google Chrome、Edge 等瀏覽器組態進行 (5) 個人防火牆設定：檢測 Windows 防火牆公用設定檔、私人設定檔、網域設定檔等組態 (6) 目前檢測範圍包含作業系統組態及部份瀏覽器組態(不包含 Mozilla Firefox)，網通設備組態及應用程式組態未在支援範圍內。 (7) 目前版本對於 Windows Server 版本之作業系統，僅只比對 Account settings 與 Common settings 二個共用群組原則，暫不支援比對其它伺服器角色(網域控制站、 DNS 伺服器、檔案伺服器及網頁伺服器)之專用群組原則。
	1-2	因下列軟體已進入產品生命週期末端，故停止維護對應之 GCB 檢測。基於安全性考量，建議停止使用已終止支援服務之軟體或盡速升級，以強化資安防護能力。 作業系統：Windows 7、Windows Server 2008 R2 瀏覽器：IE8、Microsoft Edge Legacy
	1-3	收集電腦安全性設定的方式，提供: ● 電腦開機、使用者登入登出時自動收集回報(給 WinMatrix Server)。
	1-4	自動比對電腦安全性設定項目與 GCB 的設定是否一致，並逐一顯示是否合規。
	1-5	當電腦安全性設定的項目不合規時，提供設定例外管理，並可做註記解說，以應對稽核單位的說明或核備。
	1-6	報表與查詢： (1) 提供所見即所得(WYSIWYG)查詢操作模式，令權責人員依實際需求，快速得到想查詢的資料，並可進行匯出(Excel、pdf 格式)。 (2) 可透過 WinMatrix 排程通知樣板，自動將檢核報表依照分權分責模式寄送給各單位的管理人員(或權責窗口)。 (3) 每個 GCB 項目名稱，皆有其對應的設定方式、標準值、與說明。 (4) 除 GCB 項目名稱、GCB 設定值、GCB 編號、電腦現況設值、是否合

		規等欄位外，報表與查詢中，尚有電腦資產的欄位，例如電腦名稱、IP、MAC、使用人、作業系統名稱、位元數、回報時間..等等，利於管理檢閱之需求。 (5) 依照管轄權限單位提供合規及不合規統計報表，了解相關作業的治理程度。
	1-7	提供多管理視角： (1) 可依安全性組態項目進行檢閱管理。 (2) 可依單位視角進行檢閱管理。 (3) 可依合規性與否進行檢閱管理。 (4) 可依電腦視角進行檢閱管理。 (5) 畫面中任一欄位皆可設置查詢(過濾)條件。 (6) 畫面中任一欄位皆可設置欄位群組，提供不同管理視角。

2022.4.8.

＊ 尚有其他選購模組，您可以連接到 http://www.simopro.com 以獲得更多資訊。

＊ 依據的 GCB 版本如下:

TWGCB-01-004_Microsoft Windows 8.1 政府組態基準說明文件 v1.7
TWGCB-01-005_Microsoft Windows 10 政府組態基準說明文件 v1.4
TWGCB-01-006_Microsoft Windows Server 2012 R2 政府組態基準說明文件 v1.2
TWGCB-01-007_Microsoft Windows Server 2016 政府組態基準說明文件 v1.2
TWGCB-01-009_Microsoft Windows Server 2019 政府組態基準說明文件 v1.0
TWGCB-02-002_Microsoft Internet Explorer 11 政府組態基準說明文件 v1.3
TWGCB-02-003_Google Chrome 政府組態基準說明文件 v1.4
TWGCB-02-006_Microsoft Edge 政府組態基準說明文件 v1.0

＊ 可被支援檢核的作業系統如下：

Windows 8.1、Windows 10、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019

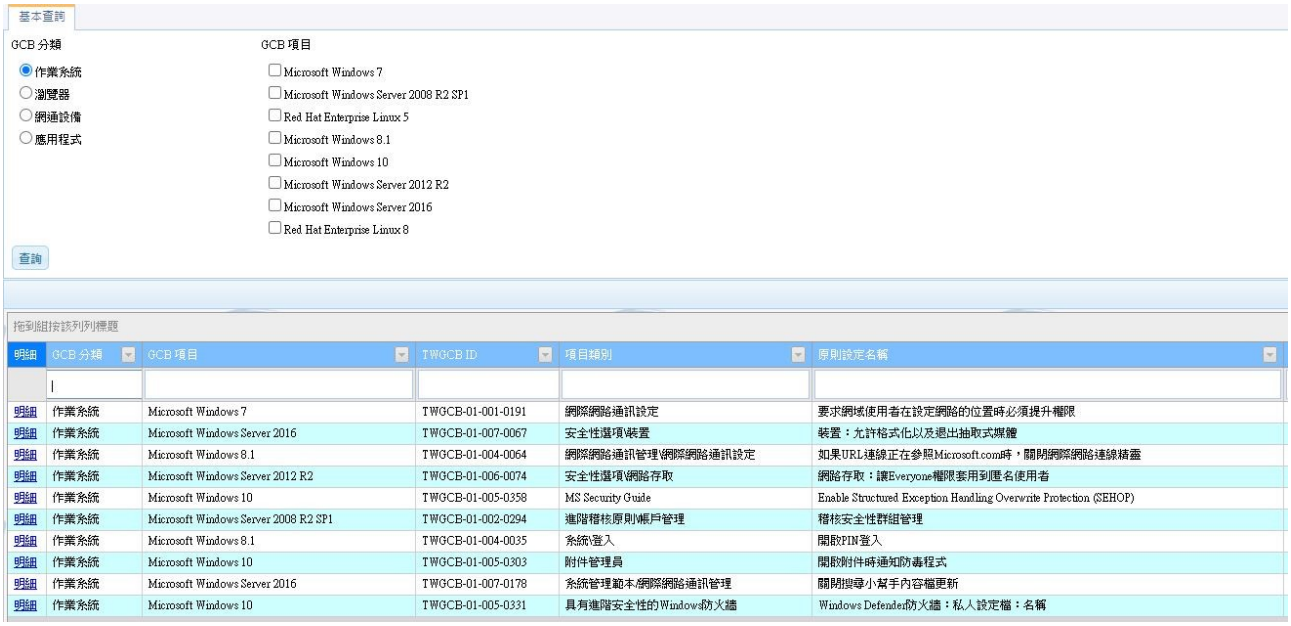
＊ 可被支援檢核的瀏覽器如下：

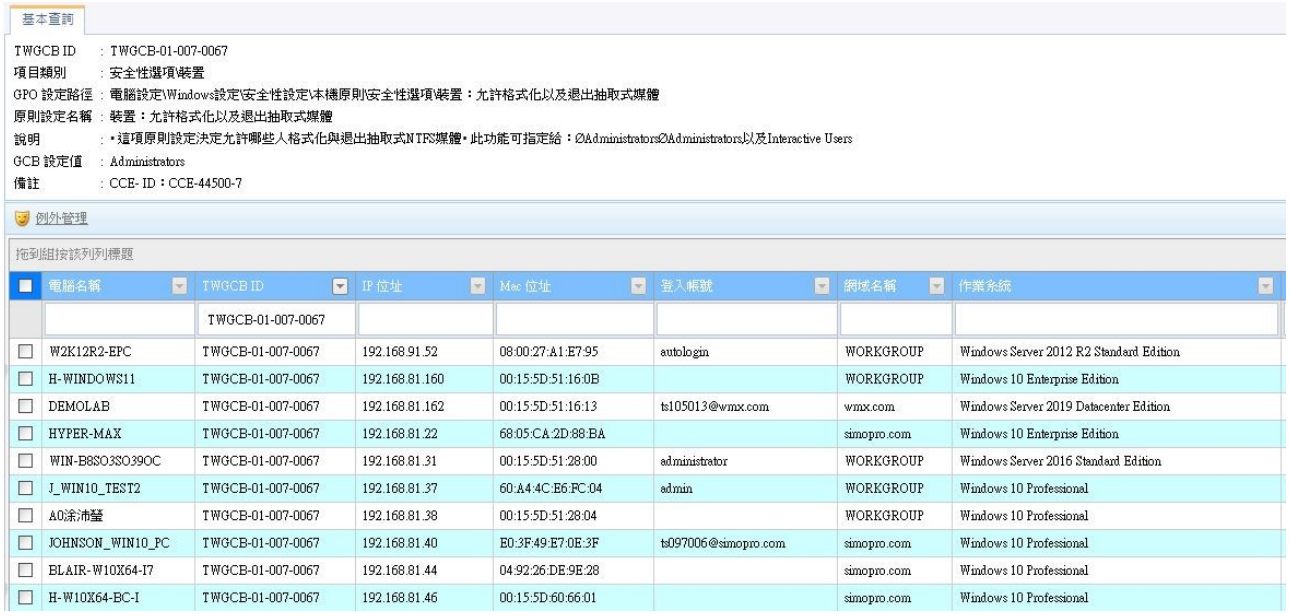
Internet Explorer 11、Microsoft Edge、Google Chrome。（不支援 Internet Explorer 8、Mozilla Firefox）

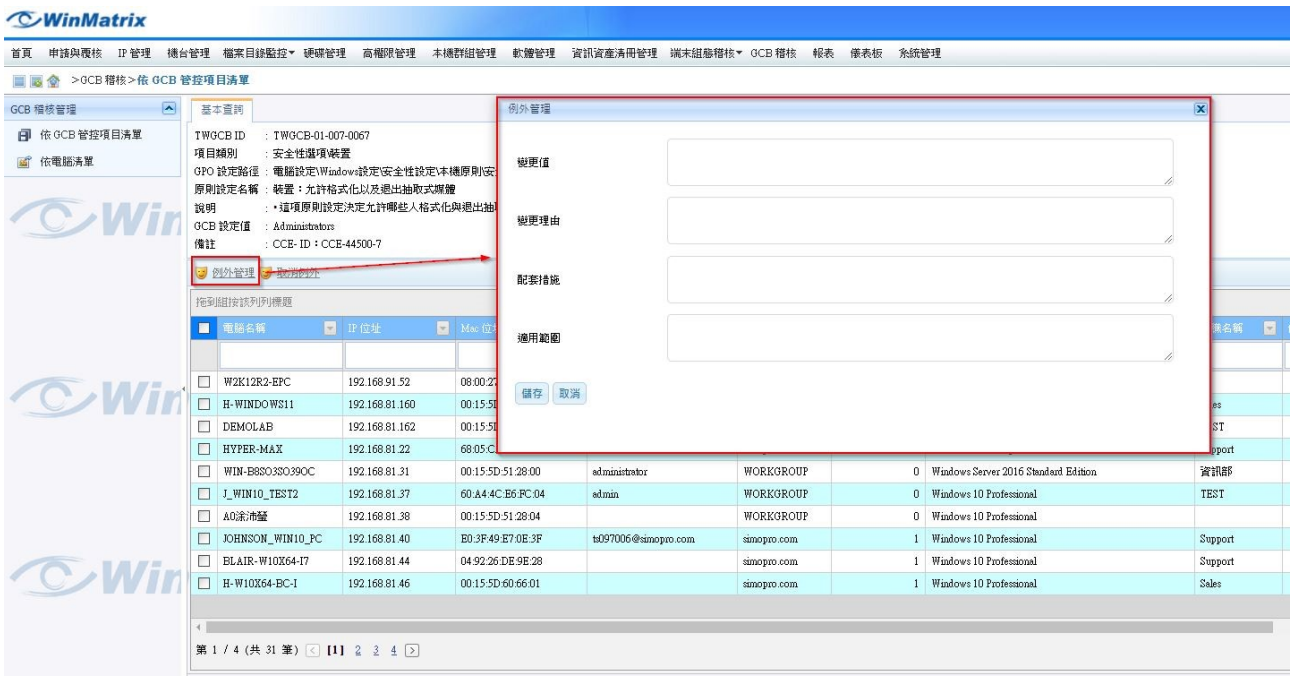
＊尚未支援的 GCB 類別項目如下：

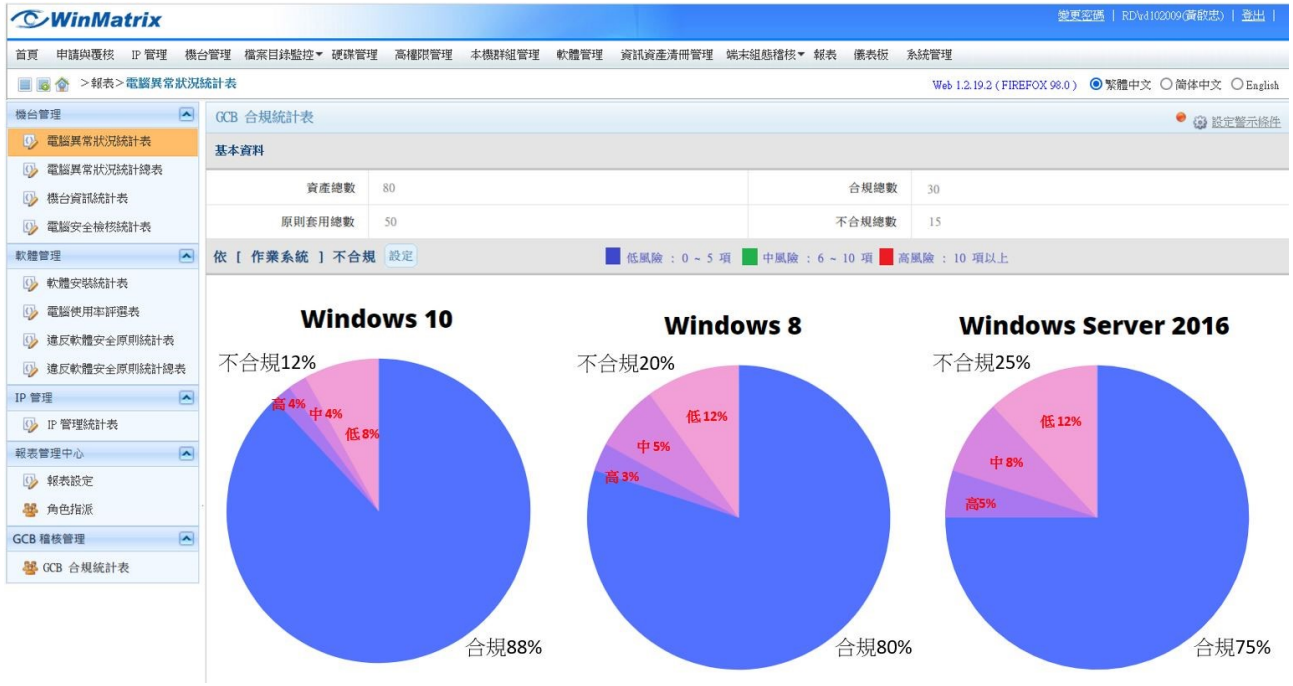
網通設備類：無線網路、Juniper Firewall、Fortinet Fortigate、Cisco Firewall。
應用程式類：Exchange Server 2013、Microsoft IIS 8.5、Word 2016、PowerPoint 2016、Excel 2016、Outlook 2016、Apache HTTP Server 2.4、Microsoft SQL Server 2016。

系統範例畫面：


基本查詢
GCB 分類
GCB 項目
作業系統
瀏覽器
網通設備
應用程式
Microsoft Windows 7
Microsoft Windows Server 2008 R2 SP1
Red Hat Enterprise Linux 5
Microsoft Windows 8.1
Microsoft Windows 10
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2016
Red Hat Enterprise Linux 8
查詢
拖到組按該列列標題
明細 GCB 分類 GCB 項目 TWGCB ID 項目類別 原則設定名稱
明細 作業系統 Microsoft Windows 7 TWGCB-01-001-0191 網際網路通訊設定 要求網域使用者在設定網路的位置時必須提升權限
明細 作業系統 Microsoft Windows Server 2016 TWGCB-01-007-0067 安全性選項\裝置 裝置：允許格式化以及退出抽取式媒體
明細 作業系統 Microsoft Windows 8.1 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
明細 作業系統 Microsoft Windows Server 2012 R2 TWGCB-01-006-0074 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
明細 作業系統 Microsoft Windows 10 TWGCB-01-005-0358 MS Security Guide Enable Structured Exception Handling Overwrite Protection (SEHOP)
明細 作業系統 Microsoft Windows Server 2008 R2 SP1 TWGCB-01-002-0294 進階稽核原則\帳戶管理 稽核安全性群組管理
明細 作業系統 Microsoft Windows 8.1 TWGCB-01-004-0035 系統\登入 開啟PIN登入
明細 作業系統 Microsoft Windows 10 TWGCB-01-005-0303 附件管理員 開啟附件時通知防毒程式
明細 作業系統 Microsoft Windows Server 2016 TWGCB-01-007-0178 系統管理範本/網際網路通訊管理 關閉搜尋小幫手內容檔更新
明細 作業系統 Microsoft Windows 10 TWGCB-01-005-0331 具有進階安全性的Windows防火牆 Windows Defender防火牆：私人設定檔：名稱


基本查詢
TWGCB ID ：TWGCB-01-007-0067
項目類別 ：安全性選項\裝置
GPO 設定路徑 ：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\裝置：允許格式化以及退出抽取式媒體
原則設定名稱 ：裝置：允許格式化以及退出抽取式媒體
說明 ：•這項原則設定決定允許哪些人格式化與退出抽取式NTFS媒體。此功能可指定給：ØAdministratorsØAdministrators以及Interactive Users
GCB 設定值 ：Administrators
備註 ：CCE- ID：CCE-44500-7
例外管理
拖到組按該列列標題
電腦名稱 TWGCB ID IP 位址 Mac 位址 登入帳號 網域名稱 作業系統
TWGCB-01-007-0067
W2K12R2-EPC TWGCB-01-007-0067 192.168.91.52 08:00:27:A1:E7:95 autologin WORKGROUP Windows Server 2012 R2 Standard Edition
H-WINDOWS11 TWGCB-01-007-0067 192.168.81.160 00:15:5D:51:16:0B WORKGROUP Windows 10 Enterprise Edition
DEMOLAB TWGCB-01-007-0067 192.168.81.162 00:15:5D:51:16:13 ts105013@wmx.com wmx.com Windows Server 2019 Datacenter Edition
HYPER-MAX TWGCB-01-007-0067 192.168.81.22 68:05:CA:2D:88:BA simopro.com Windows 10 Enterprise Edition
WIN-B8SO3SO39OC TWGCB-01-007-0067 192.168.81.31 00:15:5D:51:28:00 administrator WORKGROUP Windows Server 2016 Standard Edition
J_WIN10_TEST2 TWGCB-01-007-0067 192.168.81.37 60:A4:4C:E6:FC:04 admin WORKGROUP Windows 10 Professional
A0涂沛瑩 TWGCB-01-007-0067 192.168.81.38 00:15:5D:51:28:04 WORKGROUP Windows 10 Professional
JOHNSON_WIN10_PC TWGCB-01-007-0067 192.168.81.40 E0:3F:49:E7:0E:3F ts097006@simopro.com simopro.com Windows 10 Professional
BLAIR-W10X64-I7 TWGCB-01-007-0067 192.168.81.44 04:92:26:DE:9E:28 simopro.com Windows 10 Professional
H-W10X64-BC-I TWGCB-01-007-0067 192.168.81.46 00:15:5D:60:66:01 simopro.com Windows 10 Professional


WinMatrix
例外管理
變更值
變更理由
配套措施
適用範圍
儲存
取消


WinMatrix
GCB 合規統計表
基本資料
Windows 10
不合規12%
合規88%
Windows 8
不合規20%
合規80%
Windows Server 2016
不合規25%
合規75%