(Government Configuration Baseline，GCB)

政府組態基準導入與檢測

GCB 導入與檢測

- 作業系統:

  Windows 7 、Windows 8.1、Windows 10、Windows 11
  Server 2008 R2、Server 2012 R2、Server 2016、
  Server 2019/Server 2022

- 瀏覽器:

  IE8、IE11、Google Chrome、Mozilla Firefox、Edge

- MS Office

  Word 2016/2019、Excel 2016/2019、PowerPoint 2016/2019、
  Outlook 2016

GCB 檢測 (不包含導入)

- 作業系統:

  Red Hat Enterprise Linux 8

  CentOS 7、8

- Web Server:

  Microsoft IIS 8.5 (Windows)

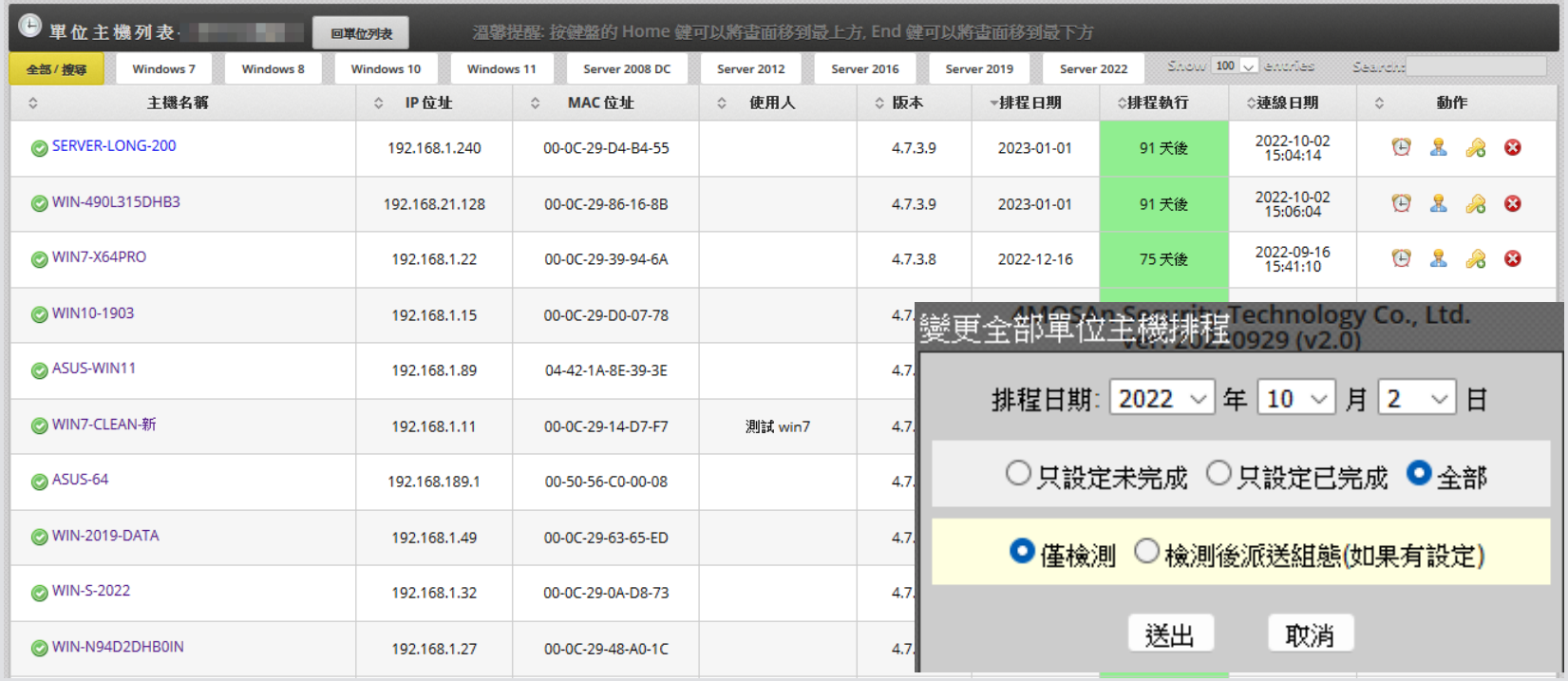
  Apache HTTP Server 2.4

  (Red Hat、CentOS Linux)

4MOSAn 美麗島安全科技

4MOSAn 美麗島安全科技

排程檢測: 可設定 [整個單位]
於排程日期進行檢測以及套用組態。



排程檢測: 可設定 [單一用戶]
於排程日期進行檢測以及套用組態。

4MOSAn 美麗島安全科技

主機資產管理

- 已排程電腦列表匯出與匯入.xlsx (Excel 檔案)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	新主機名稱	單位名稱	使用者	e-mail	組態群組	工作群組	IP 位址	MAC	作業系統	bit	原註	Mainboard	CPU	RAM	HardDisk
2	ASUS-64				test	HOME	192.168.189.1	00-50-56-C0-0	Windows 7 Pr	64		ASUSTeK C(	Intel(	16 GBy	磁碟: C 磁
3	ASUS-WIN11					HOME	192.168.1.89	04-42-1A-8E-3	Windows 10 H	64		ASUSTeK C(	11th G	16 GBy	磁碟: C 磁
4	DESKTOP-61EQU0D					WORKGROUP	192.168.1.14	88-D7-F6-C4-E	Windows 10 P	64		ASUSTeK C(	AMD I	32 GBy	磁碟: C 磁
5	SERVER-LONG-200					TEST	192.168.1.240	00-0C-29-D4-E	Windows Serv	32		VMware, In	11th G	1 GByt	磁碟: C 磁
6	VM-WIN81					HOME	192.168.1.5	00-0C-29-07-7	Windows 8.1 E	32		VMware, In	11th G	1 GByt	磁碟: C 磁
7	WIN-2019-DATA					HOME	192.168.1.49	00-0C-29-63-6	Windows Serv	64		VMware, In	11th G	8 GByt	磁碟: C 磁
8	WIN-490L315DHB3					WORKGROUP	192.168.21.128	00-0C-29-86-1	Windows Serv	64		VMware, In	11th G	2 GByt	磁碟: C 磁
9	WIN-N94D2DHB0IN					WORKGROUP	192.168.1.27	00-0C-29-48-A	Windows Serv	64		VMware, In	11th G	2 GByt	磁碟: C 磁
10	WIN-S-2022					WORKGROUP	192.168.1.32	00-0C-29-0A-D	Windows Serv	64		VMware, In	11th G	2 GByt	磁碟: C 磁
11	WIN-TGSK9K74R18					WORKGROUP	192.168.1.41	00-0C-29-CB-F	Windows Serv	64		VMware, In	11th G	2 GByt	磁碟: C 磁
12	WIN10-1903														
13	WIN7-CLEAN														
14	WIN7-X64PR														

組態設定與套用-驗證


4MOSAn GCB 政府組態基準管理中心 v2.0
使用者:
設定 登出
儀錶板
排程
軟體資產
報表
GCB 統計
組態
軟體派送
維護
Linux
幫助
[組態] 單位組態設定 - [Demo(測試)]
回單位列表
回上一頁
組態派送紀錄
溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以將畫面移到最下方
Windows 7 + IE8
Windows 7 + IE11
Windows 8 + IE11
Windows 10 + IE11
Server 2008 DC
Server 2012
Server 2016
Server 2019
全單位驗證組態
Windows 10
篩選組態群組 :
全部
套用組態至已勾選主機
選擇組態:
未指定 (清除組態套用)
送出
組態列表
新增組態 (Windows 10)
例外項目 (Windows 10)
套用組態至 Windows 10 全部主機
Show 100 entries
Search:
主機名稱
IP
組態群組
作業系統
IE
組態
狀態
動作
WIN10-1903
192.168.1.15
Windows 10 Pro 1909 Build 18363 (x64)
IE11
WIN10_office
2022-09-16 21:00 已套用
組態驗證
驗證符合
DESKTOP-61EQU0D
192.168.1.14
Windows 10 Pro (21H2) Build 19044 (x64)
IE11
未指定
ASUS-WIN11
192.168.1.89
Windows 10 Home (21H2) Build 22000 (x64)
IE11
未指定
Showing 1 to 3 of 3 entries
Previous 1 Next

組態 – 先設定例外項目

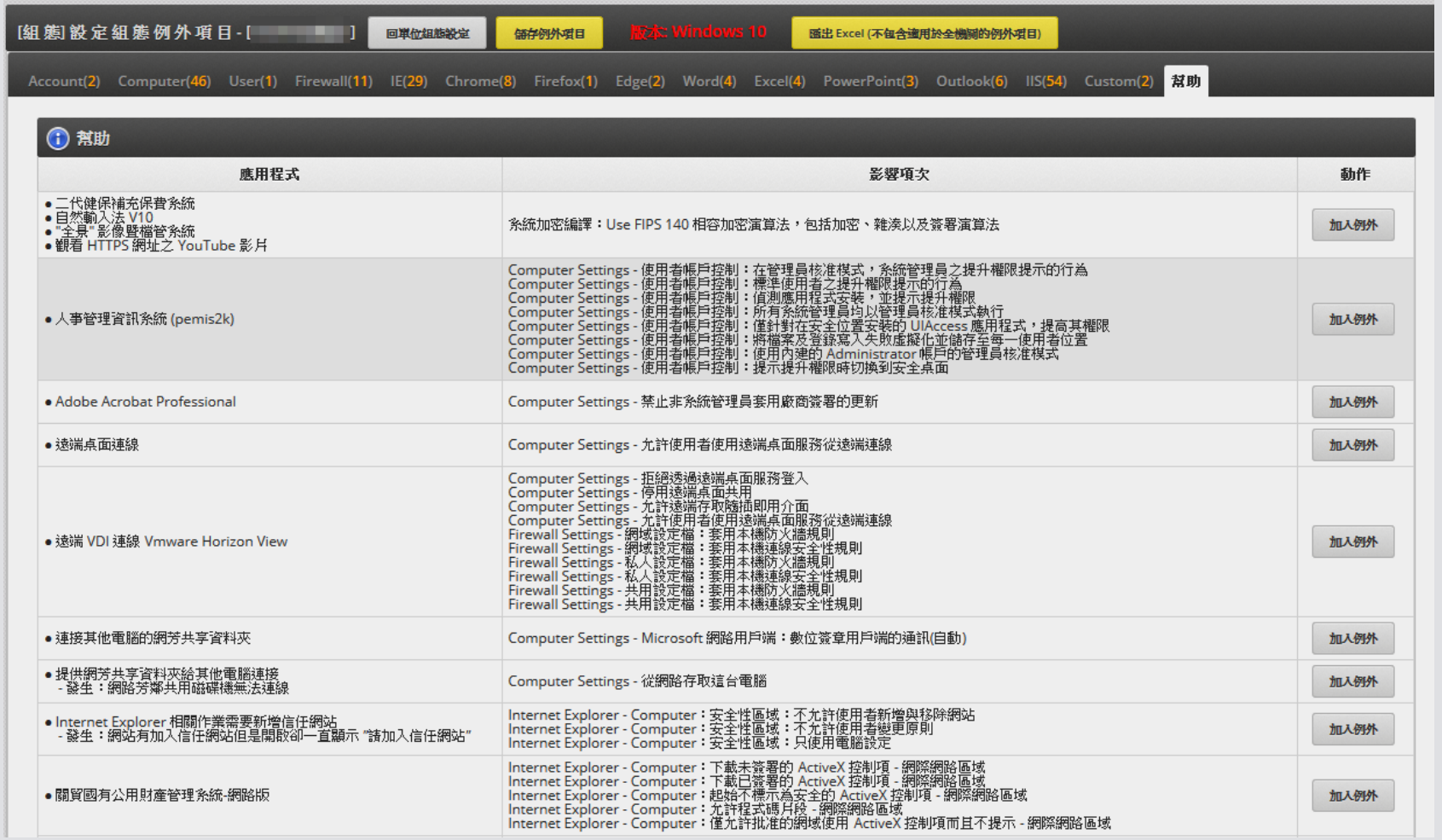
[組態] 設定組態例外項目 [redacted] 回單位組態設定 儲存例外項目 版本: Windows 10 匯出 Excel (不包含適用於全機關的例外項目)

Account(2) Computer(46) User(1) Firewall(11) IE(29) Chrome(8) Firefox(1) Edge(2) Word(4) Excel(4) PowerPoint(3) Outlook(6) IIS(54) Custom(2) 幫助

Firewall Settings - 項目數: 33

	項次	GPO	TWGCB-ID	類別	原則設定名稱	例外說明 / 影響
☐	313	Firewall Settings	TWGCB-01-005-0313	具有進階安全性的 Windows 防火牆	網域設定檔：Windows 防火牆：禁止通知	
☐	314	Firewall Settings	TWGCB-01-005-0314	具有進階安全性的 Windows 防火牆	網域設定檔：Windows 防火牆：禁止單點傳送回應到多點傳送或廣播要求	影響 1: DHCP 自動取得 IP 影響 2: 連線 WiFi 時顯示無網際網路
☑	315	Firewall Settings	TWGCB-01-005-0315	具有進階安全性的 Windows 防火牆	網域設定檔：套用本機防火牆規則 - 管理員設為全機關例外	影響 1: 遠端 VDI 連線 Vmware Horizon View 影響 2: FTP 存取檔案 影響 3: 事務機掃描的檔案回傳至電腦 影響 4: 神網系統 影響 5: 全景文件影像管理系統
☑	316	Firewall Settings	TWGCB-01-005-0316	具有進階安全性的 Windows 防火牆	網域設定檔：套用本機連線安全性規則 - 管理員設為全機關例外	影響 1: 遠端 VDI 連線 Vmware Horizon View 影響 2: FTP 存取檔案 影響 3: 事務機掃描的檔案回傳至電腦 影響 4: 神網系統
☐	317	Firewall Settings	TWGCB-01-005-0317	具有進階安全性的 Windows 防火牆	網域設定檔：輸出連線	
☐	318	Firewall Settings	TWGCB-01-005-0318	具有進階安全性的 Windows 防火牆	網域設定檔：輸入連線	
☐	319	Firewall Settings	TWGCB-01-005-0319	具有進階安全性的 Windows 防火牆	網域設定檔：記錄丟棄的封包	
☐	320	Firewall Settings	TWGCB-01-005-0320	具有進階安全性的 Windows 防火牆	網域設定檔：記錄成功的連線	
☐	321	Firewall Settings	TWGCB-01-005-0321	具有進階安全性的 Windows 防火牆	網域設定檔：大小限制	
☐	322	Firewall Settings	TWGCB-01-005-0322	具有進階安全性的 Windows 防火牆	網域設定檔：名稱	
☑	323	Firewall Settings	TWGCB-01-005-0323	具有進階安全性的 Windows 防火牆	網域設定檔：防火牆狀態 - 管理員設為全機關例外	影響 1: FTP 存取檔案 影響 2: 事務機掃描的檔案回傳至電腦 影響 3: 神網系統
☐	324	Firewall Settings	TWGCB-01-005-0324	具有進階安全性的 Windows 防火牆	私人設定檔：顯示通知	

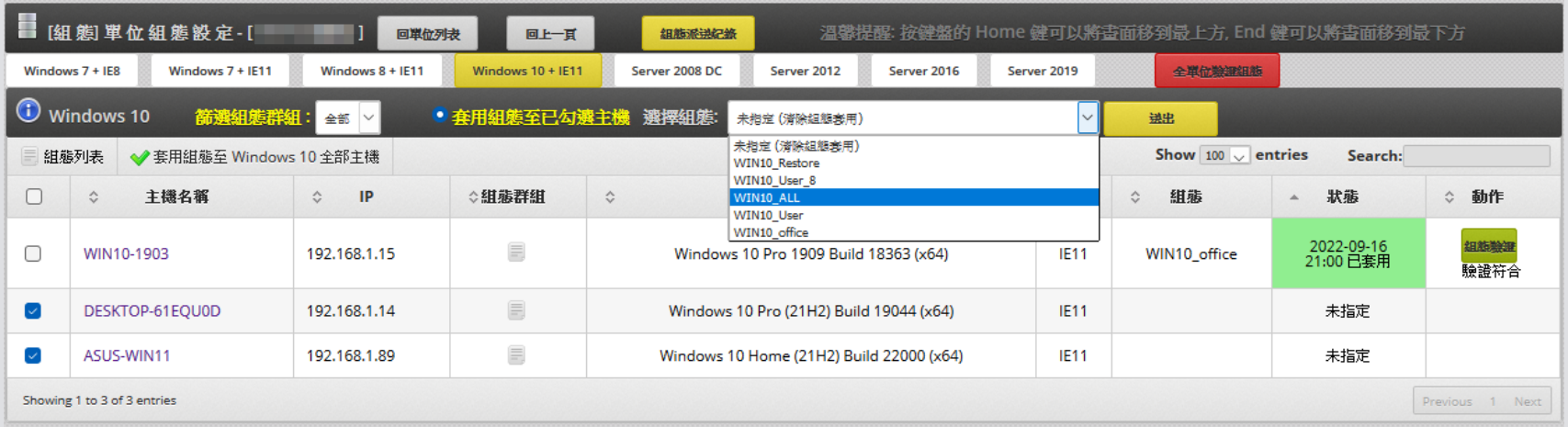
組態 – 快速設定例外項目


[組態] 設定組態例外項目 - [ ]
回單位組態設定
儲存例外項目
版本: Windows 10
匯出 Excel (不包含適用於全機關的例外項目)
Account(2) Computer(46) User(1) Firewall(11) IE(29) Chrome(8) Firefox(1) Edge(2) Word(4) Excel(4) PowerPoint(3) Outlook(6) IIS(54) Custom(2) 幫助
幫助
應用程式
影響項次
動作
• 二代健保補充保費系統
• 自然輸入法 V10
• "全景" 影像暨檔管系統
• 觀看 HTTPS 網址之 YouTube 影片
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
加入例外
• 人事管理資訊系統 (pemis2k)
Computer Settings - 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
Computer Settings - 使用者帳戶控制：標準使用者之提升權限提示的行為
Computer Settings - 使用者帳戶控制：偵測應用程式安裝，並提示提升權限
Computer Settings - 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
Computer Settings - 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
Computer Settings - 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
Computer Settings - 使用者帳戶控制：使用內建的 Administrator 帳戶的管理員核准模式
Computer Settings - 使用者帳戶控制：提示提升權限時切換到安全桌面
加入例外
• Adobe Acrobat Professional
Computer Settings - 禁止非系統管理員套用廠商簽署的更新
加入例外
• 遠端桌面連線
Computer Settings - 允許使用者使用遠端桌面服務從遠端連線
加入例外
• 遠端 VDI 連線 Vmware Horizon View
Computer Settings - 拒絕透過遠端桌面服務登入
Computer Settings - 停用遠端桌面共用
Computer Settings - 允許遠端存取隨插即用介面
Computer Settings - 允許使用者使用遠端桌面服務從遠端連線
Firewall Settings - 網域設定檔：套用本機防火牆規則
Firewall Settings - 網域設定檔：套用本機連線安全性規則
Firewall Settings - 私人設定檔：套用本機防火牆規則
Firewall Settings - 私人設定檔：套用本機連線安全性規則
Firewall Settings - 共用設定檔：套用本機防火牆規則
Firewall Settings - 共用設定檔：套用本機連線安全性規則
加入例外
• 連接其他電腦的網芳共享資料夾
Computer Settings - Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)
加入例外
• 提供網芳共享資料夾給其他電腦連接
- 發生：網路芳鄰共用磁碟機無法連線
Computer Settings - 從網路存取這台電腦
加入例外
• Internet Explorer 相關作業需要新增信任網站
- 發生：網站有加入信任網站但是開啟卻一直顯示 "請加入信任網站"
Internet Explorer - Computer：安全性區域：不允許使用者新增與移除網站
Internet Explorer - Computer：安全性區域：不允許使用者變更原則
Internet Explorer - Computer：安全性區域：只使用電腦設定
加入例外
• 關貿國有公用財產管理系統-網路版
Internet Explorer - Computer：下載未簽署的 ActiveX 控制項 - 網際網路區域
Internet Explorer - Computer：下載已簽署的 ActiveX 控制項 - 網際網路區域
Internet Explorer - Computer：起始不標示為安全的 ActiveX 控制項 - 網際網路區域
Internet Explorer - Computer：允許程式碼片段 - 網際網路區域
Internet Explorer - Computer：僅允許批准的網域使用 ActiveX 控制項而且不提示 - 網際網路區域
加入例外

組態 – 新增組態(勾選)

	項次	GPO	TWGCB-ID	類別	原則設定名稱	影響
☑	10	Computer Settings	TWGCB-01-005-0010	控制台\個人化	防止啟用鎖定畫面相機	
☑	11	Computer Settings	TWGCB-01-005-0011	控制台\個人化	防止啟用鎖定畫面投影片放映	
☑	12	Computer Settings	TWGCB-01-005-0012	網路\網路連線	要求網域使用者在設定網路的位置時必須提升權限	
☑	13	Computer Settings	TWGCB-01-005-0013	網路\網路連線	禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接	
☐	14	Computer Settings	TWGCB-01-005-0014	網路\網路連線	透過內部網路路由傳送所有流量 - 例外項目	沒有說明
☑	15	Computer Settings	TWGCB-01-005-0015	網路\網路提供者	已強化的 UNC 路徑	
☐	16	Computer Settings	TWGCB-01-005-0016	網路\Windows 連線管理員	最小化網際網路或 Windows 網域的同時連線數目 - 例外項目	沒有說明
☑	17	Computer Settings	TWGCB-01-005-0017	網路\Windows 連線管理員	當連線到通過網域驗證的網路時，禁止連線到非網域網路	
☑	18	Computer Settings	TWGCB-01-005-0018	網路\連結階層拓撲搜尋	開啟 Mapper I/O(LLTDIO) 驅動程式	
☑	19	Computer Settings	TWGCB-01-005-0019	網路\連結階層拓撲搜尋	開啟 Responder(RSPNDR) 驅動程式	
☐	20	Computer Settings	TWGCB-01-005-0020	網路\Lanman 工作站	啟用不安全的來賓登入 - 例外項目	影響 NAS 網芳分享磁碟
☑	21	Computer Settings	TWGCB-01-005-0021	網路\Microsoft 對等網路服務	關閉 Microsoft 對等網路服務	
☑	22	Computer Settings	TWGCB-01-005-0022	網路\TCP 設定值	設定 6to4 狀態	
☑	23	Computer Settings	TWGCB-01-005-0023	網路\TCPIP 設定值	設定 IP-HTTPS 狀態	
☑	24	Computer Settings	TWGCB-01-005-0024	網路\TCP 設定值\IPv6 轉換技術	設定 ISATAP 狀態	

組態 – 套用



依照各作業系統設定 [例外項目]、[導入的項目]
前期可以先小規模套用組態，進行測試，調整
之後再批次進行導入

套用名稱為 **Restore** 組態，可以將主機恢復到原本的組態設定狀態 (從備份檔進行回復)

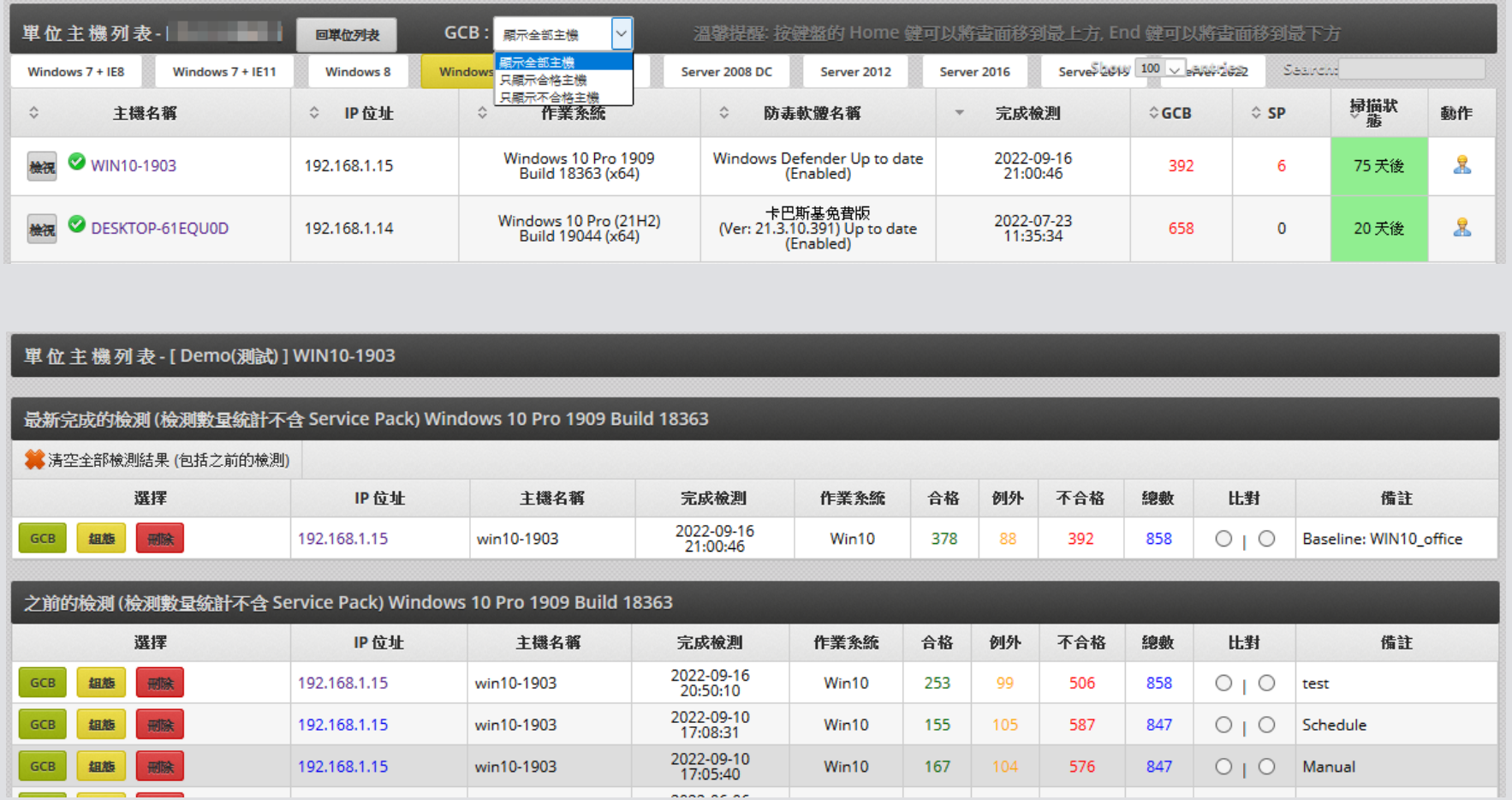
組態派送: 保留一年內的派送紀錄

4MOSAn 美麗島安全科技

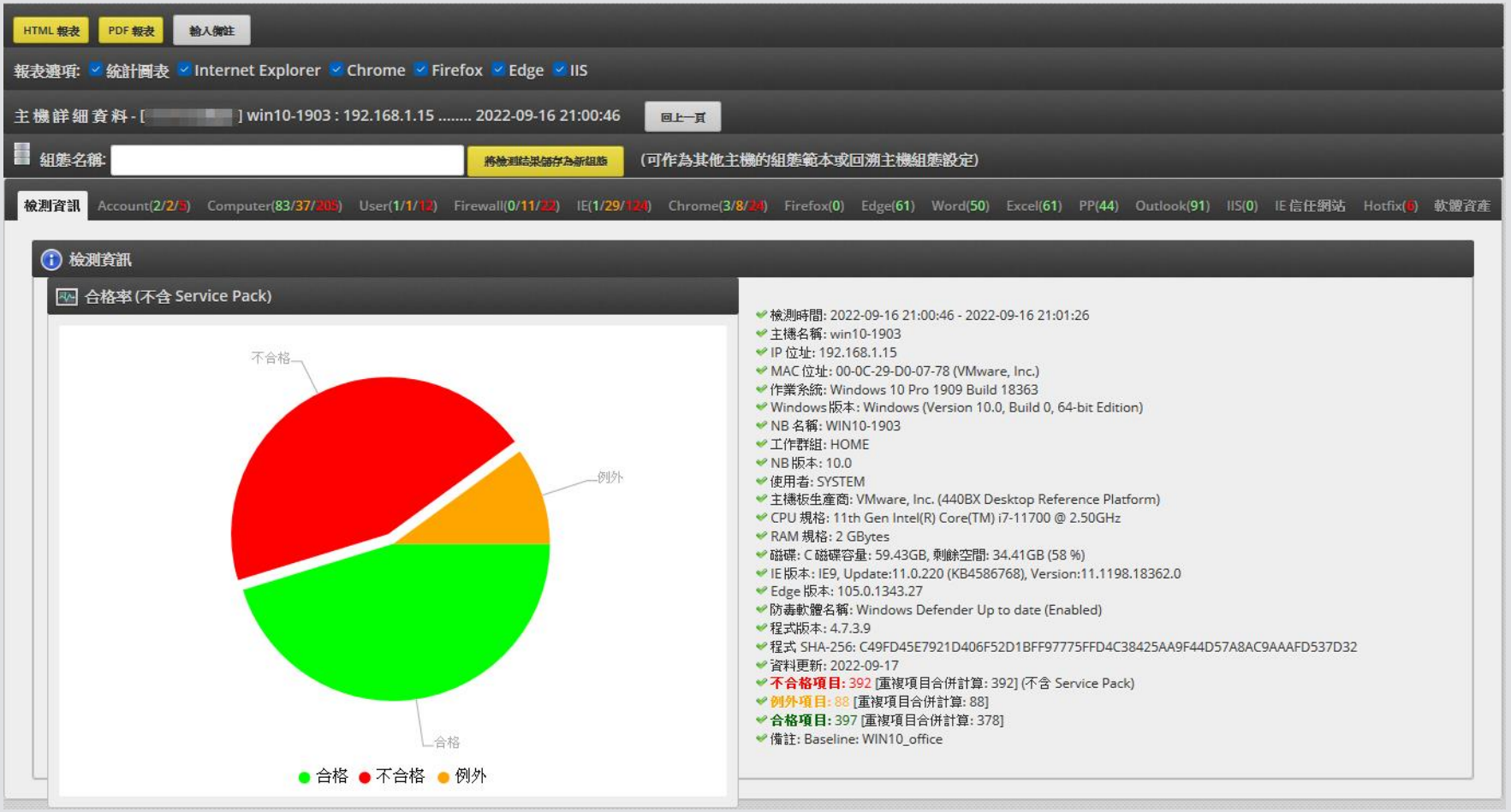
GCB 檢測報表

4MOSAn 美麗島安全科技

GCB 檢測報表

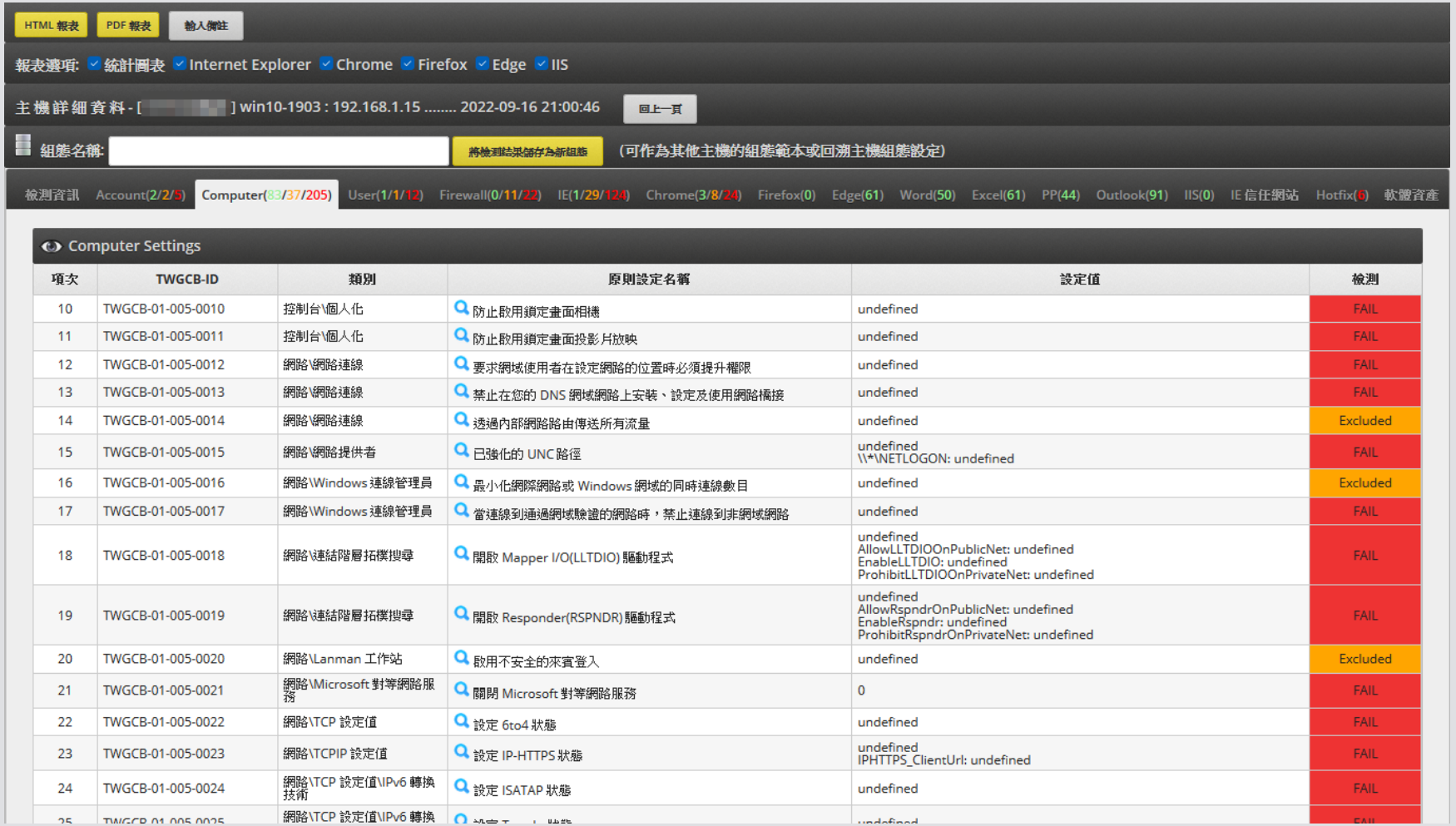


GCB 檢測報表


HTML 報表
PDF 報表
輸入備註
報表選項: 統計圖表 Internet Explorer Chrome Firefox Edge IIS
主機詳細資料 - [ ] win10-1903 : 192.168.1.15 ..... 2022-09-16 21:00:46
回上一頁
組態名稱:
將檢測結果儲存為新組態
(可作為其他主機的組態範本或回溯主機組態設定)
檢測資訊 Account(2/2/5) Computer(83/37/205) User(1/1/12) Firewall(0/11/22) IE(1/29/124) Chrome(3/8/24) Firefox(0) Edge(61) Word(50) Excel(61) PP(44) Outlook(91) IIS(0) IE 信任網站 Hotfix(6) 軟體資產
檢測資訊
合格率 (不含 Service Pack)
不合格
例外
合格
合格 不合格 例外
檢測時間: 2022-09-16 21:00:46 - 2022-09-16 21:01:26
主機名稱: win10-1903
IP 位址: 192.168.1.15
MAC 位址: 00-0C-29-D0-07-78 (VMware, Inc.)
作業系統: Windows 10 Pro 1909 Build 18363
Windows 版本: Windows (Version 10.0, Build 0, 64-bit Edition)
NB 名稱: WIN10-1903
工作群組: HOME
NB 版本: 10.0
使用者: SYSTEM
主機板生產商: VMware, Inc. (440BX Desktop Reference Platform)
CPU 規格: 11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz
RAM 規格: 2 GBytes
磁碟: C 磁碟容量: 59.43GB, 剩餘空間: 34.41GB (58 %)
IE 版本: IE9, Update:11.0.220 (KB4586768), Version:11.1198.18362.0
Edge 版本: 105.0.1343.27
防毒軟體名稱: Windows Defender Up to date (Enabled)
程式版本: 4.7.3.9
程式 SHA-256: C49FD45E7921D406F52D1BFF97775FFD4C38425AA9F44D57A8AC9AAAFD537D32
資料更新: 2022-09-17
不合格項目: 392 [重複項目合併計算: 392] (不含 Service Pack)
例外項目: 88 [重複項目合併計算: 88]
合格項目: 397 [重複項目合併計算: 378]
備註: Baseline: WIN10_office

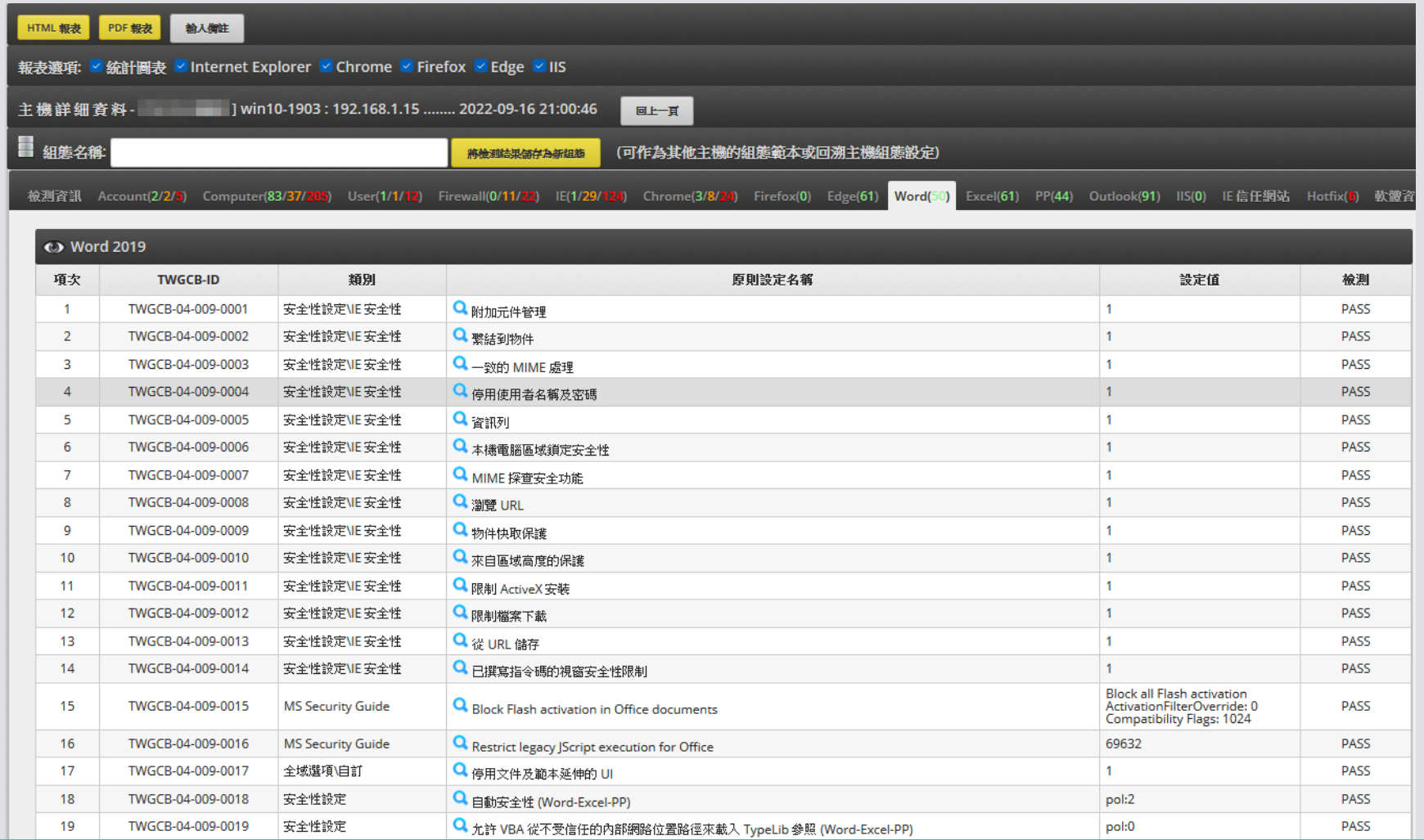
4MOSAn 美麗島安全科技

GCB 檢測報表



項次	TWGCB-ID	類別	原則設定名稱	設定值	檢測
10	TWGCB-01-005-0010	控制台\個人化	防止啟用鎖定畫面相機	undefined	FAIL
11	TWGCB-01-005-0011	控制台\個人化	防止啟用鎖定畫面投影片放映	undefined	FAIL
12	TWGCB-01-005-0012	網路\網路連線	要求網域使用者在設定網路的位置時必須提升權限	undefined	FAIL
13	TWGCB-01-005-0013	網路\網路連線	禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接	undefined	FAIL
14	TWGCB-01-005-0014	網路\網路連線	透過內部網路路由傳送所有流量	undefined	Excluded
15	TWGCB-01-005-0015	網路\網路提供者	已強化的 UNC 路徑	undefined *\NETLOGON: undefined	FAIL
16	TWGCB-01-005-0016	網路\Windows 連線管理員	最小化網際網路或 Windows 網域的同時連線數目	undefined	Excluded
17	TWGCB-01-005-0017	網路\Windows 連線管理員	當連線到通過網域驗證的網路時，禁止連線到非網域網路	undefined	FAIL
18	TWGCB-01-005-0018	網路\連結階層拓撲搜尋	開啟 Mapper I/O(LLTDIO) 驅動程式	undefined AllowLLTDIOOnPublicNet: undefined EnableLLTDIO: undefined ProhibitLLTDIOOnPrivateNet: undefined	FAIL
19	TWGCB-01-005-0019	網路\連結階層拓撲搜尋	開啟 Responder(RSPNDR) 驅動程式	undefined AllowRspndrOnPublicNet: undefined EnableRspndr: undefined ProhibitRspndrOnPrivateNet: undefined	FAIL
20	TWGCB-01-005-0020	網路\Lanman 工作站	啟用不安全的來賓登入	undefined	Excluded
21	TWGCB-01-005-0021	網路\Microsoft 對等網路服務	關閉 Microsoft 對等網路服務	0	FAIL
22	TWGCB-01-005-0022	網路\TCP 設定值	設定 6to4 狀態	undefined	FAIL
23	TWGCB-01-005-0023	網路\TCPIP 設定值	設定 IP-HTTPS 狀態	undefined IPHTTPS_ClientUrl: undefined	FAIL
24	TWGCB-01-005-0024	網路\TCP 設定值\IPv6 轉換技術	設定 ISATAP 狀態	undefined	FAIL
25	TWGCB-01-005-0025	網路\TCP 設定值\IPv6 轉換			

GCB 檢測報表



Word 2019

項次	TWGCB-ID	類別	原則設定名稱	設定值	檢測
1	TWGCB-04-009-0001	安全性設定\IE 安全性	附加元件管理	1	PASS
2	TWGCB-04-009-0002	安全性設定\IE 安全性	繫結到物件	1	PASS
3	TWGCB-04-009-0003	安全性設定\IE 安全性	一致的 MIME 處理	1	PASS
4	TWGCB-04-009-0004	安全性設定\IE 安全性	停用使用者名稱及密碼	1	PASS
5	TWGCB-04-009-0005	安全性設定\IE 安全性	資訊列	1	PASS
6	TWGCB-04-009-0006	安全性設定\IE 安全性	本機電腦區域鎖定安全性	1	PASS
7	TWGCB-04-009-0007	安全性設定\IE 安全性	MIME 探查安全功能	1	PASS
8	TWGCB-04-009-0008	安全性設定\IE 安全性	瀏覽 URL	1	PASS
9	TWGCB-04-009-0009	安全性設定\IE 安全性	物件快取保護	1	PASS
10	TWGCB-04-009-0010	安全性設定\IE 安全性	來自區域高度的保護	1	PASS
11	TWGCB-04-009-0011	安全性設定\IE 安全性	限制 ActiveX 安裝	1	PASS
12	TWGCB-04-009-0012	安全性設定\IE 安全性	限制檔案下載	1	PASS
13	TWGCB-04-009-0013	安全性設定\IE 安全性	從 URL 儲存	1	PASS
14	TWGCB-04-009-0014	安全性設定\IE 安全性	已撰寫指令碼的視窗安全性限制	1	PASS
15	TWGCB-04-009-0015	MS Security Guide	Block Flash activation in Office documents	Block all Flash activation ActivationFilterOverride: 0 Compatibility Flags: 1024	PASS
16	TWGCB-04-009-0016	MS Security Guide	Restrict legacy JScript execution for Office	69632	PASS
17	TWGCB-04-009-0017	全域選項\自訂	停用文件及範本延伸的 UI	1	PASS
18	TWGCB-04-009-0018	安全性設定	自動安全性 (Word-Excel-PP)	pol:2	PASS
19	TWGCB-04-009-0019	安全性設定	允許 VBA 從不受信任的內部網路位置路徑來載入 TypeLib 參照 (Word-Excel-PP)	pol:0	PASS

單主機 GCB 報告
HTML/PDF 格式

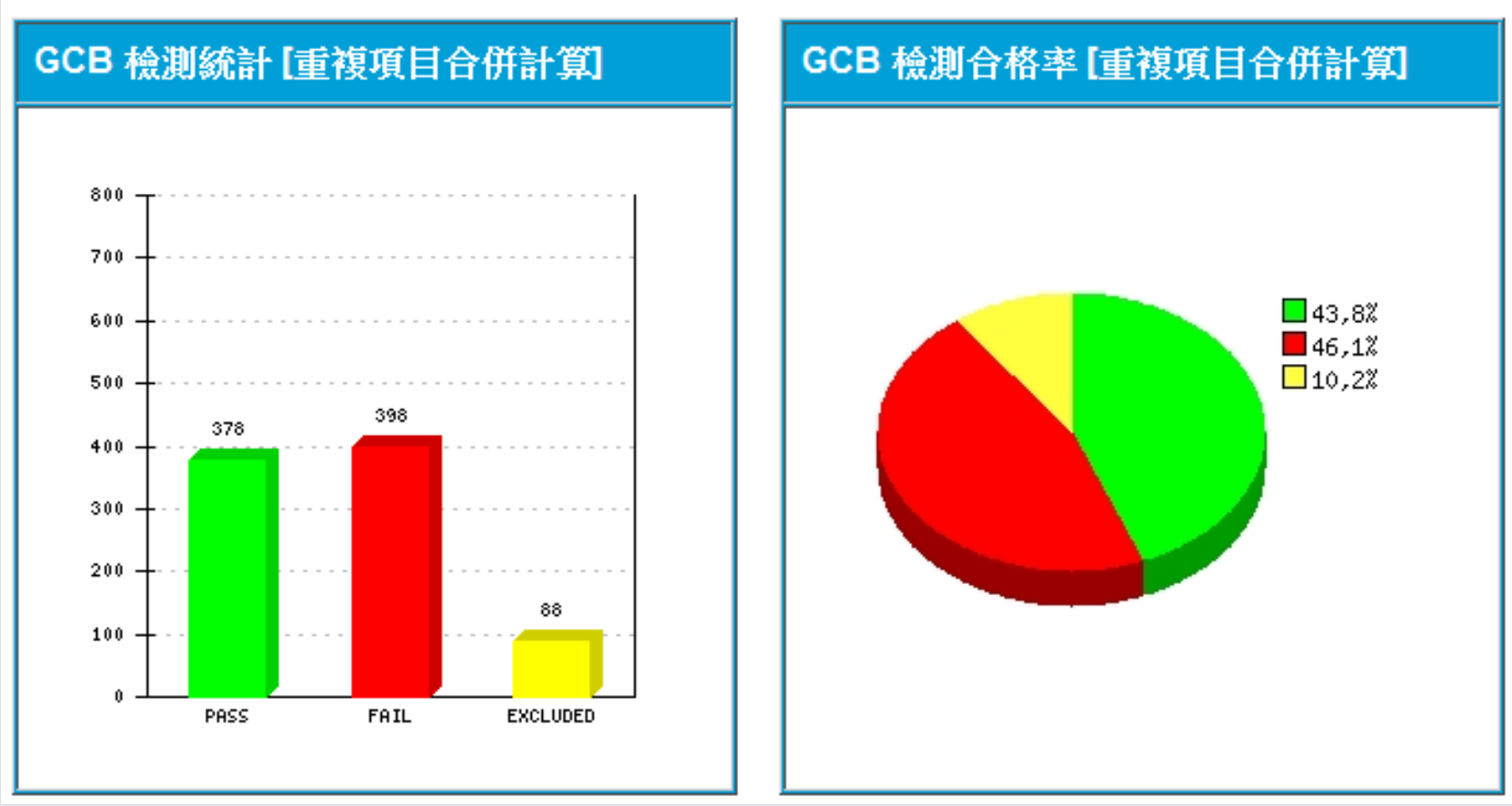
GCB 檢測報告 HTML/PDF

4MOSAn GCB 政府組態基準

資訊

開始時間: 2022/09/16 21:00:46 - 2022/09/16 21:01:26
主機名稱: win10-1903
IP 位址: 192.168.1.15
MAC / 閘道: 00-0C-29-D0-07-78
MAC 供應商: VMware, Inc.
作業系統: Windows 10 Pro 1909 x64
Windows 版本: Windows (Version 10.0, Build 0, 64-bit Edition)
電腦名稱: WIN10-1903
工作群組: HOME
NetBIOS 版本: 10.0
主機規格: VMware, Inc. (440BX Desktop Reference Platform)
使用者: SYSTEM
CPU 規格: 11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz
RAM 規格: 2 GBytes
磁碟: C 磁碟容量: 59.43GB, 剩餘空間: 34.41GB (58 %)
IE 版本: IE9, Update:11.0.220 (KB4586768), Version:11.1198.18362.0
Edge 版本: 105.0.1343.27
防毒軟體名稱: Windows Defender Up to date (Enabled)
稽核程式版本: 4.7.3.9
資料更新日期: 2022-09-17

GCB 檢測報告 HTML/PDF



GCB 檢測報告 HTML/PDF

檢測摘要

編號	群組	合格	不合格	已排除	Total
1	Account Policy	2	5	2	9
2	Computer Settings	83	205	37	325
3	User Settings	1	12	1	14
4	Firewall Settings	0	22	11	33
5	Internet Explorer	1	124	29	154
6	Google Chrome	3	24	8	35
7	Mozilla Firefox	0	0	0	0
8	Edge	61	0	0	61
9	IIS	0	0	0	0
10	Word	50	0	0	50
11	Excel	61	0	0	61
12	PowerPoint	44	0	0	44
13	Outlook	91	0	0	91
14	Custom	0	0	0	0

GCB 檢測報告 HTML/PDF

規則摘要

Account Policy		FAIL
1 - 1	TWGCB-01-005-0001 密碼最短使用期限 Value: 0	FAIL
1 - 3	TWGCB-01-005-0003 最小密碼長度 Value: 0	EXCLUDED
1 - 4	TWGCB-01-005-0004 密碼必須符合複雜性需求 Value: 0	FAIL
1 - 5	TWGCB-01-005-0005 強制執行密碼歷程記錄 Value: 0	EXCLUDED
1 - 7	TWGCB-01-005-0007 帳戶鎖定閾值 Value: 0	FAIL
1 - 8	TWGCB-01-005-0008 重設帳戶鎖定計數器的時間間隔 Value: 30	FAIL
1 - 9	TWGCB-01-005-0009 帳戶鎖定期間 (帳戶鎖定時間) Value: 30	FAIL

Computer Settings		FAIL
2 - 10	TWGCB-01-005-0010 防止啟用鎖定畫面相機 Value: undefined	FAIL

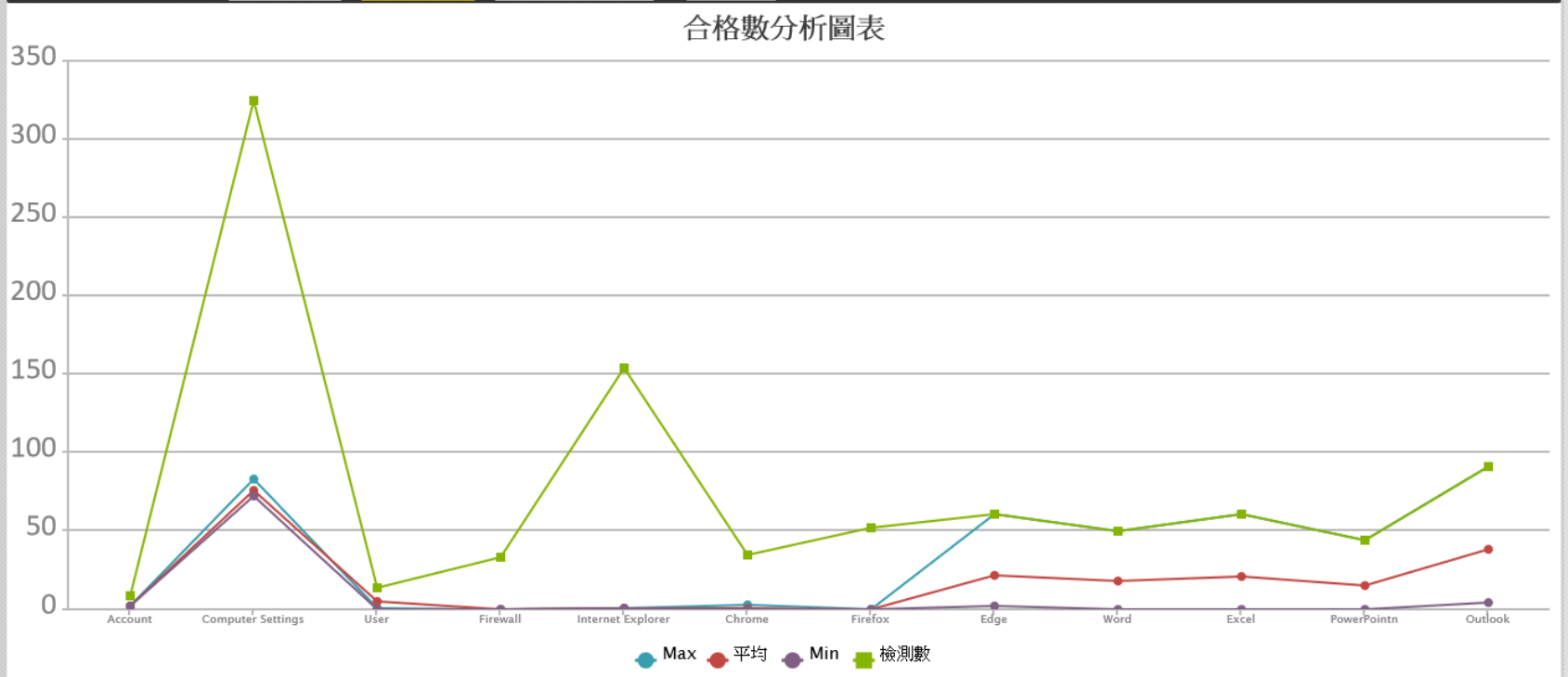
GCB 統計 – 合格數分析列表

檢測電腦數	區分	Account Policy	Computer Settings	User Settings	Firewall Settings	Internet Explorer	Google Chrome	Mozilla Firefox	Edge	Word	Excel	PP	Outlook	總檢測數	
3	檢測數	9	325	14	33	154	35	52	61	50	61	44	91	929	
主機名稱	IP 位址	Account Policy	Computer Settings	User Settings	Firewall Settings	Internet Explorer	Google Chrome	Mozilla Firefox	Edge	Word	Excel	PP	Outlook	總合格數	合格率
檢視 ASUS-WIN11	192.168.1.89	2	74	1	0	1	0	0	4	4	2	2	19	109	12 %
檢視 WIN10-1903	192.168.1.15	2	83	1	0	1	3	0	61	50	61	44	91	397	43 %

GCB 統計 – 合格數分析圖表

Windows 7 + IE8 | Windows 7 + IE11 | Windows 8/8.1 + IE11 | **Windows 10/11 + IE11** | Server 2008 DC | Server 2012 | Server 2016 | Server 2019

單位列表- [redacted] | 合格數分析列表 | 合格數分析圖表 | 導入前後合格數分析圖表 | 回單位列表

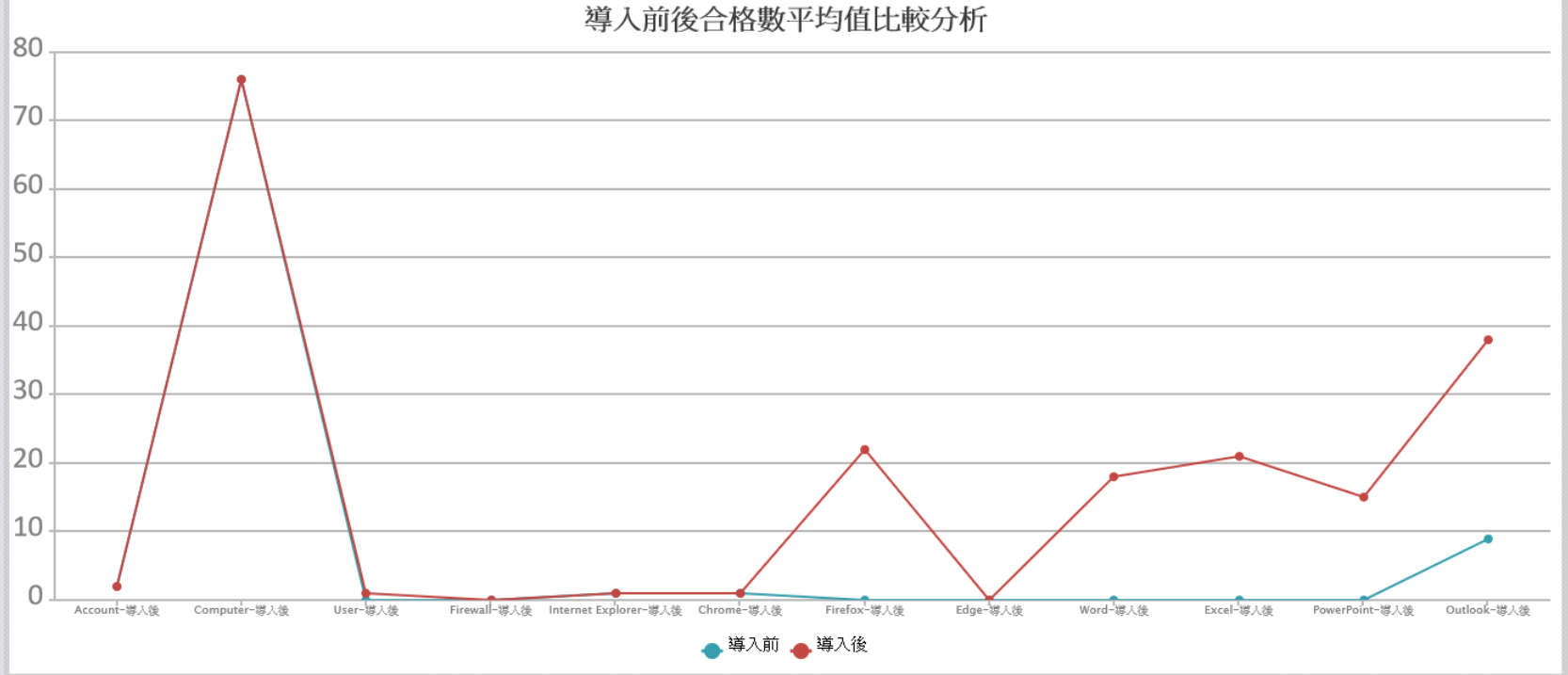


	Account Policy	Computer Settings	User Settings	Firewall Settings	Internet Explorer	Google Chrome	Mozilla Firefox	Edge	Word	Excel	PP	Outlook	總合格數
檢測數	9	325	14	33	154	35	52	61	50	61	44	91	929
平均	2	76	5	0	1	1	0	22	18	21	15	38	199
Max	2	83	1	0	1	3	0	61	50	61	44	91	397
Min	2	72	0	0	1	0	0	2	0	0	0	4	81

GCB 統計 – 導入前、後分析

Windows 7 + IE8 | Windows 7 + IE11 | Windows 8/8.1 + IE11 | Windows 10/11 + IE11 | Server 2008 DC | Server 2012 | Server 2016 | Server 2019

單位列表 - [redacted] | 合格數分析列表 | 合格數分析圖表 | 導入前後合格數分析圖表 | 回單位列表



	Account Policy	Computer Settings	User Settings	Firewall Settings	Internet Explorer	Google Chrome	Firefox	Edge	Word	Excel	PP	Outlook	總合格數
檢測數	9	325	14	33	154	35	52	61	50	61	44	91	929
導入前	2	76	0	0	1	1	0	0	0	0	0	9	89
導入後	2	76	1	0	1	1	22	0	18	21	15	38	195

GCB 檢測 (Red Hat、CentOS)

Linux 主機列表　下載 TWGCB-01-008_Red Hat Enterprise Linux 8 政府組態基準說明文件 v1.0_1100924.pdf

新增 Red Hat 主機 | Red Hat Lunix 例外項目 | Apache HTTP Server 2.4 例外項目　Show 100

報表	主機	IP 位址	主機名稱	群組	作業系統	合格	例外	不合格	總檢測數	檢測時間
Red Hat Apache	[redacted]	[redacted]	[redacted]	測試	CentOS Linux release 7.9.2009 (Core)	110	9	173	292	2022-09-08 21:49:43
Red Hat Apache	[redacted]	[redacted]	[redacted]	root	CentOS Linux release 7.9.2009 (Core)	124	10	158	292	2022-09-13 14:59:35

報表 - [[redacted] CentOS Linux release 7.9.2009 (Core) : 2022-09-08 21:49:43]　報表匯出 EXCEL 檔　回上一頁　溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以

基本項目 1-91 (98/5/140) | 基本項目 92-184 | 基本項目 185-243 | Firewalld 防火牆組態基準 (2/3) | Nftables 防火牆組態基準 (1/6) | Iptables 防火牆組態基準 (1/5) | SSH 伺服器組態基準 (8/1/22)

基本項目 1-91

例外	項次	TWGCB-ID	類別	原則設定名稱	檢測資訊	GCB 設定值	檢測
+	1	TWGCB-01-008-0001	磁碟與檔案系統	cramfs 檔案系統	exec: rmmod cramfs rmmod: ERROR: Module cramfs is not currently loaded	停用	PASS
✖	2	TWGCB-01-008-0002	磁碟與檔案系統	squashfs 檔案系統	/etc/modprobe.d/squashfs.conf: 未設定 install squashfs /bin/true 或 blacklist squashfs exec: rmmod squashfs rmmod: ERROR: Module squashfs is not currently loaded	停用	Excluded
✖	3	TWGCB-01-008-0003	磁碟與檔案系統	udf 檔案系統	exec: rmmod udf rmmod: ERROR: Module udf is not currently loaded	停用	PASS
+	4	TWGCB-01-008-0004	磁碟與檔案系統	設定 /tmp 目錄之檔案系統	/etc/fstab: tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 不存在 /etc/systemd/system/local-fs.target.wants/tmp.mount 檔案不存在	tmpfs	FAIL
+	5	TWGCB-01-008-0005	磁碟與檔案系統	設定 /tmp 目錄之 nodev 選項	/etc/fstab: 未設定 /tmp 或 ,nodev /etc/systemd/system/local-fs.target.wants/tmp.mount 檔案不存在	啟用	FAIL
+	6	TWGCB-01-008-0006	磁碟與檔案系統	設定 /tmp 目錄之 nosuid 選項	/etc/fstab: 未設定 /tmp 或 ,nosuid /etc/systemd/system/local-fs.target.wants/tmp.mount 檔案不存在	啟用	FAIL
+	7	TWGCB-01-008-0007	磁碟與檔案系統	設定 /tmp 目錄之 noexec 選項	/etc/fstab: 未設定 /tmp 或 ,noexec /etc/systemd/system/local-fs.target.wants/tmp.mount 檔案不存在	啟用	FAIL
+	8	TWGCB-01-008-0008	磁碟與檔案系統	設定 /var 目錄之檔案系統	/etc/fstab: /dev/varvg/varlv /var xfs defaults 不存在	使用獨立之分割磁區或邏輯磁區	FAIL

GCB 檢測 (Red Hat、CentOS)

報表 - [ ]: CentOS Linux release 7.9.2009 (Core) : 2022-09-08 21:49:43] 報表匯出 EXCEL 檔 回上一頁 溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以將

基本項目 1-91 (98/5/140) 基本項目 92-184 基本項目 185-243 Firewalld 防火牆組態基準 (2/3) Nftables 防火牆組態基準 (1/6) Iptables 防火牆組態基準 (1/5) SSH 伺服器組態基準 (8/1/22)

SSH 伺服器組態基準

例外	項次	TWGCB-ID	類別	原則設定名稱	檢測資訊	GCB 設定值	檢測
✚	1	TWGCB-01-008-0262	SSH 設定	sshd 守護程序	openssh-server 套件已安裝: ● sshd.service - OpenSSH server daemon Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled; vendor preset: enabled) Active: active (running) since Thu 2022-09-08 20:37:49 CST; 1h 12min ago Docs: man:sshd(8)	啟用	FAIL
✚	2	TWGCB-01-008-0263	SSH 設定	SSH 協定版本	權限不足! 無法讀取 /etc/ssh/sshd_config	Protocol 2	FAIL
✚	3	TWGCB-01-008-0264	SSH 設定	/etc/ssh/sshd_config 檔案所有權	/etc/ssh/sshd_config: -rw-------. 1 root root 4737 Aug 31 20:35 /etc/ssh/sshd_config	root:root	PASS
✚	4	TWGCB-01-008-0265	SSH 設定	/etc/ssh/sshd_config 檔案權限	/etc/ssh/sshd_config: -rw-------. 1 root root 4737 Aug 31 20:35 /etc/ssh/sshd_config	600 或更低權限	PASS
✚	5	TWGCB-01-008-0266	SSH 設定	限制存取 SSH	權限不足! 無法讀取 /etc/ssh/sshd_config	啟用	FAIL
✚	6	TWGCB-01-008-0267	SSH 設定	SSH 主機私鑰檔案所有權	私鑰檔案所有權 root:root	root:root	PASS
✚	7	TWGCB-01-008-0268	SSH 設定	SSH 主機私鑰檔案權限	私鑰檔案權限 600	600 或更低權限	PASS
✚	8	TWGCB-01-008-0269	SSH 設定	SSH 主機公鑰檔案所有權	公鑰檔案所有權 root:root	root:root	PASS
✚	9	TWGCB-01-008-0270	SSH 設定	SSH 主機公鑰檔案權限	私鑰檔案權限 644	644 或更低權限	PASS
✚	10	TWGCB-01-008-0271	SSH 設定	SSH 加密演算法	權限不足! 無法讀取 /etc/ssh/sshd_config	aes128-ctr,aes192-ctr,aes256-ctr	FAIL
✚	11	TWGCB-01-008-0272	SSH 設定	SSH 日誌記錄等級	權限不足! 無法讀取 /etc/ssh/sshd_config	VERBOSE 或 INFO	FAIL
✚	12	TWGCB-01-008-0273	SSH 設定	SSH X11Forwarding 功能	權限不足! 無法讀取 /etc/ssh/sshd_config	no	FAIL
✚	13	TWGCB-01-008-0274	SSH 設定	SSH MaxAuthTries 參數	權限不足! 無法讀取 /etc/ssh/sshd_config	4 以下，但須大於 0	FAIL
✚	14	TWGCB-01-008-0275	SSH 設定	SSH IgnoreRhosts 參數	權限不足! 無法讀取 /etc/ssh/sshd_config	yes	FAIL
✚	15	TWGCB-01-008-0276	SSH 設定	SSH HostbasedAuthentication 參數	權限不足! 無法讀取 /etc/ssh/sshd_config	no	FAIL
✖	16	TWGCB-01-008-0277	SSH 設定	SSH PermitRootLogin 參數	權限不足! 無法讀取 /etc/ssh/sshd_config	no	Excluded
✚	17	TWGCB-01-008-0278	SSH 設定	SSH PermitEmptyPasswords 參數	權限不足! 無法讀取 /etc/ssh/sshd_config	no	FAIL

GCB 檢測 (Apache 2.4)

報表 - [Apache/2.4.52 (codeit) : 2022-09-14 13:26:40] 報表匯出 EXCEL 檔 回上一頁

(53/6/5)

例外	項次	TWGCB-ID	類別	原則設定名稱	檢測資訊	GCB 設定值	檢測
+	1	TWGCB-04-007-0001	Apache 模組	Log Config 模組	LoadModule log_config_module modules/mod_log_config.so	啟用	PASS
+	2	TWGCB-04-007-0002	Apache 模組	WebDAV 模組	#LoadModule dav_module modules/mod_dav.so #LoadModule dav_fs_module modules/mod_dav_fs.so	停用	PASS
+	3	TWGCB-04-007-0003	Apache 模組	Status 模組	#LoadModule status_module modules/mod_status.so	停用	PASS
+	4	TWGCB-04-007-0004	Apache 模組	Autoindex 模組	#LoadModule autoindex_module modules/mod_autoindex.so	停用	PASS
+	5	TWGCB-04-007-0005	Apache 模組	Proxy 模組	#LoadModule proxy_module modules/mod_proxy.so	停用	PASS
+	6	TWGCB-04-007-0006	Apache 模組	User Directories 模組	#LoadModule userdir_module modules/mod_userdir.so	停用	PASS
+	7	TWGCB-04-007-0007	Apache 模組	Info 模組	#LoadModule info_module modules/mod_info.so	停用	PASS
+	8	TWGCB-04-007-0008	權限與所有權	以非 root 身分運行 Apache 網頁伺服器	User apache Group apache apache:x:48:www,ftp,apache	以非 root 身分(如 apache) 使用者與群組運行 Apache 網頁伺服器	PASS
+	9	TWGCB-04-007-0009	權限與所有權	運行 Apache 網頁伺服器之帳戶禁止登入系統	apache:x:48:48:Apache:/usr /share/httpd:/sbin/nologin	禁止登入系統	PASS
+	10	TWGCB-04-007-0010	權限與所有權	鎖定運行 Apache 網頁伺服器之帳戶密碼	apache LK 2015-06-24 -1 -1 -1 -1 (Password locked.)	鎖定密碼	PASS
+	11	TWGCB-04-007-0011	權限與所有權	設定 Apache 目錄與檔案之擁有者	root	root	PASS
+	12	TWGCB-04-007-0012	權限與所有權	設定 Apache 目錄與檔案之所屬群組	root	root	PASS
+	13	TWGCB-04-007-0013	權限與所有權	設定 Apache 目錄與檔案之 others 身分權限	755, drwxr-xr-x.	others 身分不具寫入權限	PASS
+	14	TWGCB-04-007-0014	權限與所有權	限制 Apache 目錄與檔案之群組寫入權限	755, drwxr-xr-x.	群組不具寫入權限	PASS
✖	15	TWGCB-04-007-0015	權限與所有權	限制文件根目錄與檔案之群組寫入權限		運行 Apache 網頁伺服器之群組不具有寫入權限	Excluded
+	16	TWGCB-04-007-0016	權限與所有權	保護核心轉儲目錄	無 CoreDumpDirectory 設定	目錄所有權設為「root: 運行 Apache 伺服器群組(例如 apache)」所擁有，並移除 others 權限	PASS
+	17	TWGCB-04-007-0017	權限與所有權	保護鎖定檔案	Mutex posixsem	目錄位於本機硬碟，且所有權設為「root:root」與僅由啟動 Apache 的帳戶 (例如 root)具寫入權限	PASS
+	18	TWGCB-04-007-0018	權限與所有權	保護 pid 檔案	無 pidFile 設定	目錄所有權設為「root:root」與僅由啟動 Apache 的帳戶 (例如 root)具寫入權限	PASS

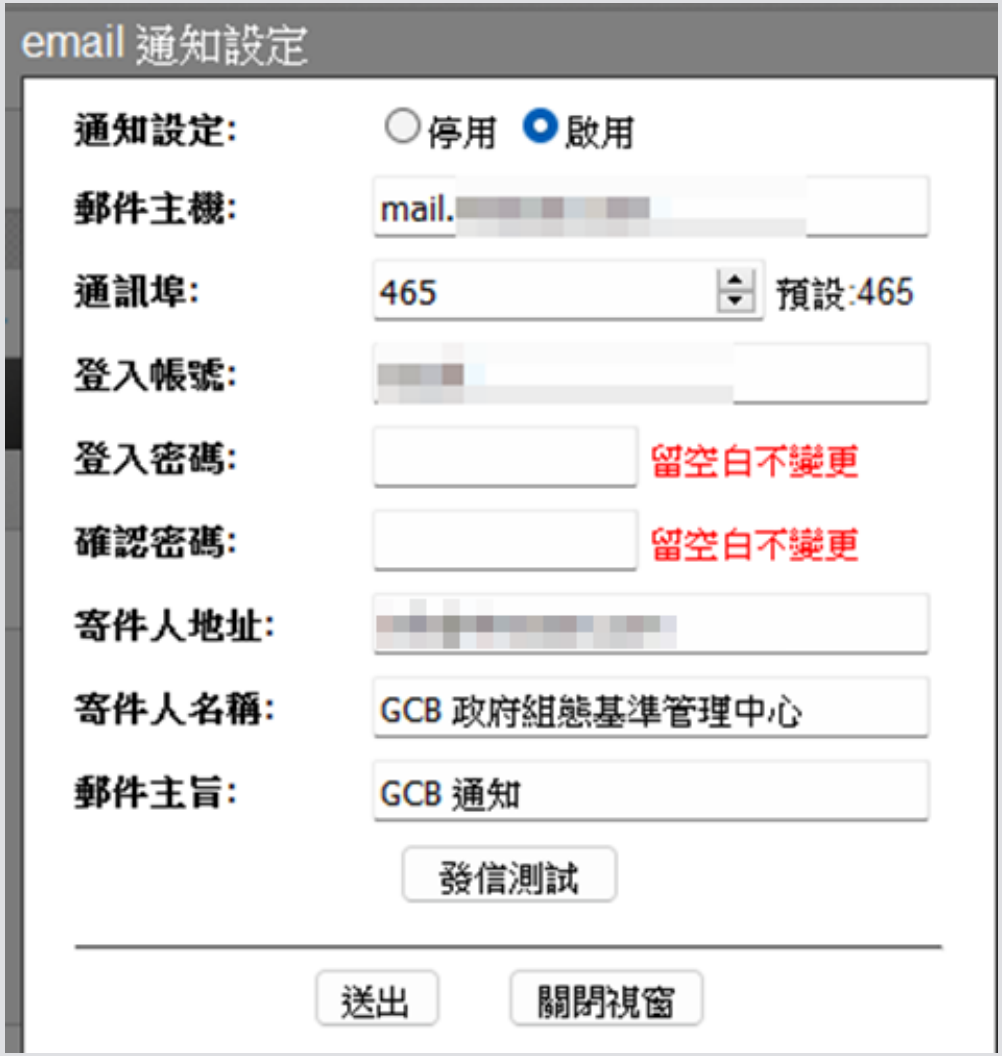
管理中心-軟體資產

單位軟體統計-[redacted] 匯出軟體統計列表 回單位列表 溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以將畫面移到最下方

軟體統計 黑名單軟體 Show 100 entries Search:

數量	軟體名稱	版本
12	4MOSAn 政府組態基準設定與檢測 4.1	4.1
9	4MOSAn 分散式弱點管理 4.0	4.0
7	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	9.0.30729.4148
6	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	9.0.30729.6161
4	Microsoft Edge Update	1.3.167.21
4	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	9.0.30729.6161
4	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219
3	Microsoft Visual C++ 2005 Redistributable	8.0.61001
3	Microsoft Visual C++ 2005 Redistributable (x64)	8.0.61000
3	Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022	9.0.21022
3	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219
3	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	12.0.30501.0
3	VMware Tools	10.0.0.2977863
2	7-Zip 18.05 (x64)	18.05
2	Adobe Refresh Manager	1.8.0
2	Advanced Installer 11.9	11.9

Email 設定


email 通知設定
通知設定:
停用
啟用
郵件主機:
mail.
通訊埠:
465
預設:465
登入帳號:
登入密碼:
留空白不變更
確認密碼:
留空白不變更
寄件人地址:
寄件人名稱:
GCB 政府組態基準管理中心
郵件主旨:
GCB 通知
發信測試
送出
關閉視窗

Email 通知

寄件者: GCB 政府組態基準管理中心 [redacted]

收件者: [redacted]

副本:

主旨: GCB 通知

GCB 組態檢測完成通知

檢測單位: [redacted]
檢測主機: WIN-490L315DHB3
檢測時間: 2022-10-02 15:06:41
檢測類型: 排程檢測
檢測間隔: 91 天
下次檢測: 2023-01-01 15:06:00
查看最新的檢測報告.
https:/[redacted]9df1b1

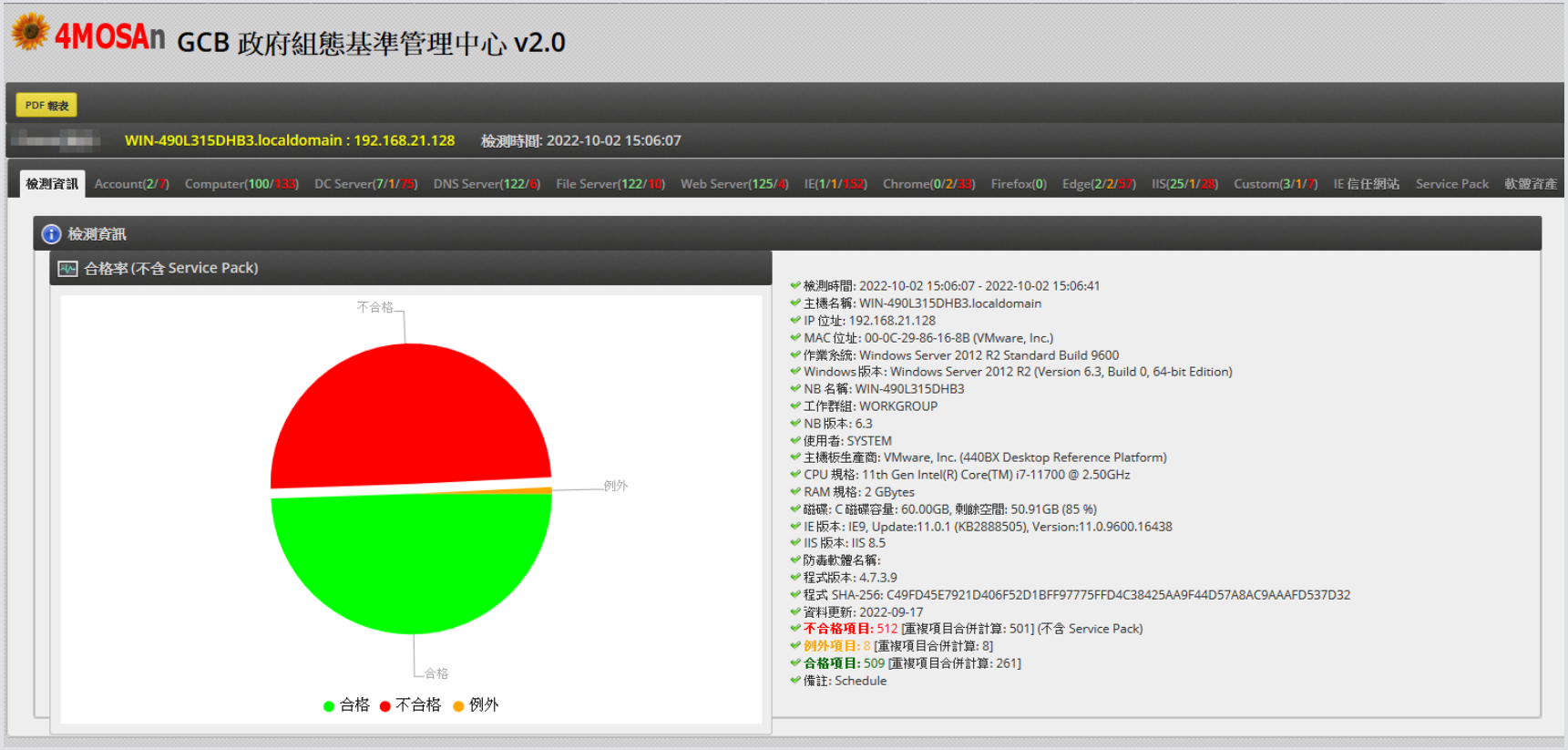
本郵件由 4MOSAn GCB 政府組態基準管理中心寄出.

Email 通知

- 組態檢測後發出通知信件給電腦列表中, 主機使用者的 E-mail
- 新增帳號、刪除帳號之後, 寄送郵件通知給相關帳號的 E-mail
- 帳號之密碼變更之後, 寄送郵件通知給相關帳號設定的 E-mail
- 設定套用組態之後, 寄送郵件通知給全部系統管理員以及全部單位管理員的 E-mail
- 設定派送軟體之後, 寄送郵件通知給全部系統管理員以及全部單位管理員的 E-mail

4MOSAn 美麗島安全科技

點選連結檢視報告



4MOSAn 美麗島安全科技

點選連結檢視報告

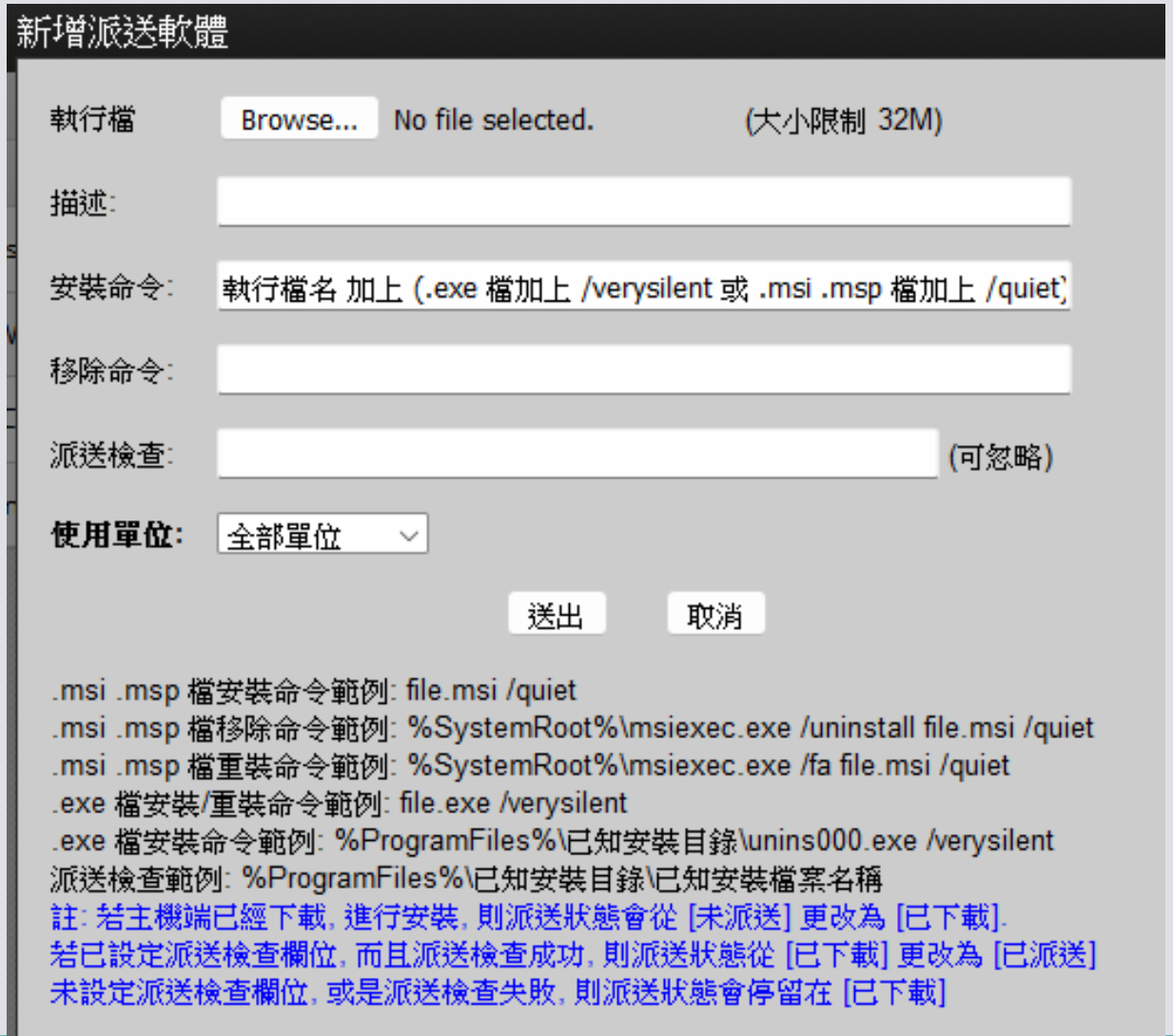
項次	GPO	TWGCB-ID	類別	原則設定名稱	設定值	檢測
10	Computer Settings	TWGCB-01-006-0010	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器	0	PASS
11	Computer Settings	TWGCB-01-006-0011	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章用戶端的通訊(如果伺服器同意)	1	PASS
12	Computer Settings	TWGCB-01-006-0012	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)	0	FAIL
13	Computer Settings	TWGCB-01-006-0013	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級	undefined	FAIL
14	Computer Settings	TWGCB-01-006-0014	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)	0	FAIL
15	Computer Settings	TWGCB-01-006-0015	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)	0	FAIL
16	Computer Settings	TWGCB-01-006-0016	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	15	PASS
17	Computer Settings	TWGCB-01-006-0017	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線	1	PASS
18	Computer Settings	TWGCB-01-006-0018	安全性選項\MSS	MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic	undefined	FAIL
19	Computer Settings	TWGCB-01-006-0019	安全性選項\MSS	MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds	undefined	FAIL
20	Computer Settings	TWGCB-01-006-0020	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	undefined	FAIL
21	Computer Settings	TWGCB-01-006-0021	安全性選項\MSS	MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	1	PASS
22	Computer Settings	TWGCB-01-006-0022	安全性選項\MSS	MSS：(Hidden) Hide computer from the browse list (Not Recommended except for highly secure environments)	undefined	FAIL

軟體派送功能

- 軟體派送功能具備密碼保護
- 允許派送 msi、exe、msp (Windows Installer Patch)

- 軟體派送紀錄: 保留一年內的紀錄
- 派送功能包括: [安裝、移除] 軟體
- 可篩選作業系統作業系統，搜尋特定弱點，
  大量派送 . msp (Windows Installer Patch) 或
  其他軟體版本升級 (如 Java SE、Acrobat Reader)

軟體派送


新增派送軟體
執行檔
Browse...
No file selected.
(大小限制 32M)
描述:
安裝命令:
執行檔名 加上 (.exe 檔加上 /verysilent 或 .msi .msp 檔加上 /quiet)
移除命令:
派送檢查:
(可忽略)
使用單位:
全部單位
送出
取消
.msi .msp 檔安裝命令範例: file.msi /quiet
.msi .msp 檔移除命令範例: %SystemRoot%\msiexec.exe /uninstall file.msi /quiet
.msi .msp 檔重裝命令範例: %SystemRoot%\msiexec.exe /fa file.msi /quiet
.exe 檔安裝/重裝命令範例: file.exe /verysilent
.exe 檔安裝命令範例: %ProgramFiles%\已知安裝目錄\unins000.exe /verysilent
派送檢查範例: %ProgramFiles%\已知安裝目錄\已知安裝檔案名稱
註: 若主機端已經下載, 進行安裝, 則派送狀態會從 [未派送] 更改為 [已下載].
若已設定派送檢查欄位, 而且派送檢查成功, 則派送狀態從 [已下載] 更改為 [已派送]
未設定派送檢查欄位, 或是派送檢查失敗, 則派送狀態會停留在 [已下載]

密碼政策與帳戶政策

- 最小密碼長度 (可自訂)
- 符合複雜性需求 (可自訂)
- 允許密碼重複使用 (可自訂)
- 密碼使用期限: (天數可自訂)

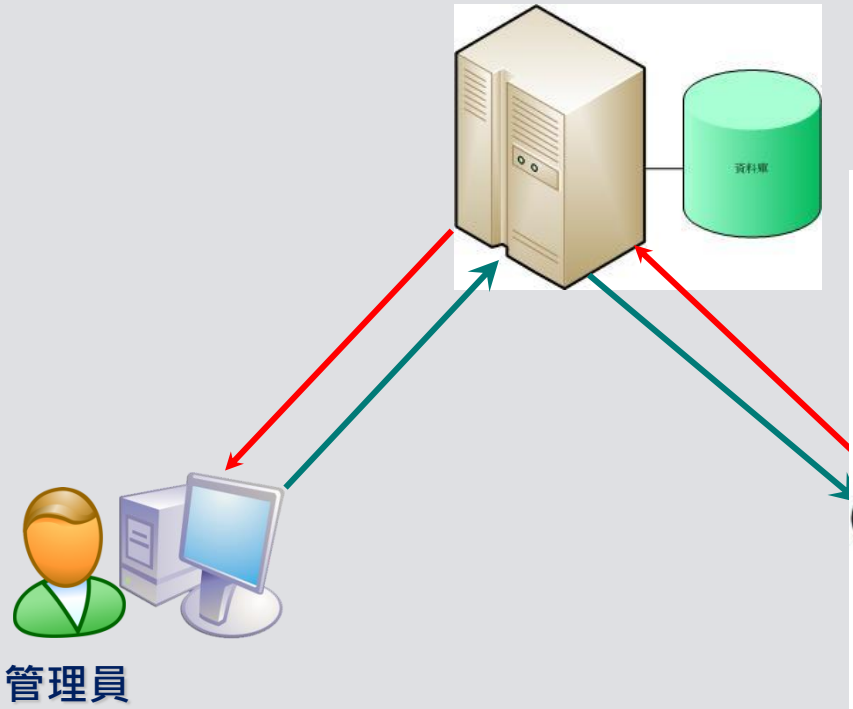
- 帳戶鎖定閾值: 5 次
- 重設帳戶鎖定計數器的時間: 15 分鐘
- 帳戶鎖定期間 (帳戶鎖定時間): 15 分鐘

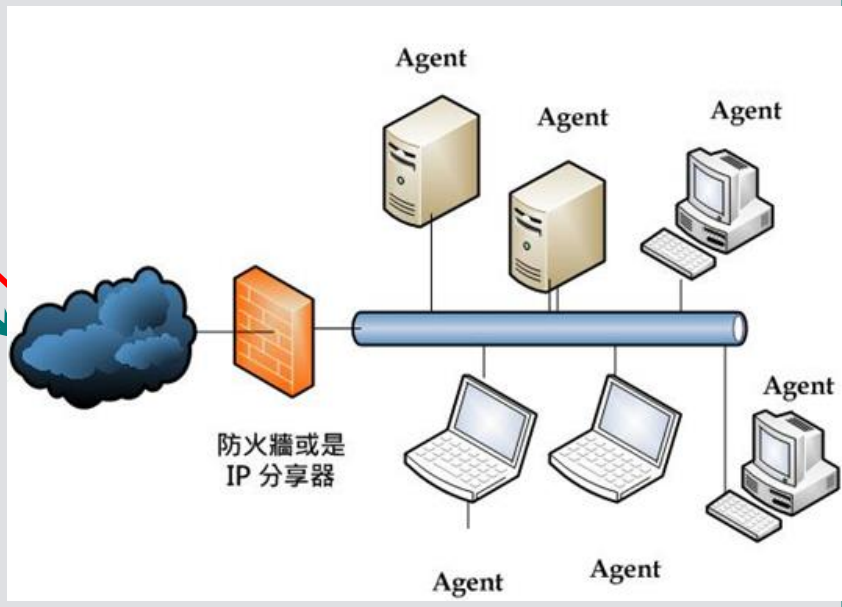
- 可限制登入 IP 位址
- 登入紀錄: 保留一年內的紀錄

支援雙重驗證 (Google Authenticator)

管理中心

- 分散檢測 + 中央集中式管理　　三層式系統架構 (3-tier)





系統包含

- **GCB 管理中心:**

  作業系統: FreeBSD 13.2

  提供檔案: 開放虛擬機器格式檔案 .OVF

  （Open Virtualization Format）

- **Windows 安裝程式:**

  提供 .msi 以及 .exe 兩種安裝程式

  支援靜默安裝 (/quiet 以及 /verysilent)

管理中心功能

- 排程檢測: 可設定 [整個單位] 或 [單一用戶] 於排程日期進行檢測。
- 報表通知: 排程檢測後，可設定以 email 通知用戶端，檢視最新的檢測報表。
- 組態設定: 備份主機原始組態設定，恢復主機原始組態設定。
- 組態設定: 可設定適用於全機關的例外項目，以及個別機關的的例外項目。
- 組態設定: 可強制要求下次登入時變更密碼 (取消密碼永久有效)。
- 組態設定: 可只套用有勾選的組態項目，不變更未勾選的組態項目設定值。
- 組態設定: 支援客製化組態，可依照單位需要，加入 TW-GCB 以外的組態項目進行檢測與套用。

管理中心功能

- 組態派送: 可設定多個組態檔，針對不同使用功能的用戶派送合適的組態檔。
- 組態派送: 機關主機可設定不同的組態群組，組態派送可選擇只派送至某一個組態群組。
- 組態派送: 組態套用後，回傳檢測結果，可設定以 email 通知用戶端，檢視最新的檢測報表。
- 組態派送: 組態套用後，可驗證套用的組態與組態檢測結果是否符合。
- 報表檢視: 可檢視每一次完成檢測的日期時間、合格數量、例外數量、不合格數量、檢測總數。
- 報表檢視: 可檢視組態檢測項目的合格率，以及每一項目的檢測狀態 (PASS/FAIL) 與項目說明。

管理中心功能

- 報表檢視: 可選擇兩次檢測結果進行比對，列出兩次檢測的組態差異項目。
- 報表檢視: 可篩選 只顯示合格主機/只顯示不合格主機，快速列出總體(合格/不合格) 的主機。
- 報表檢視: 可搜尋特定組態項目(合格/不合格)，快速列出單一項目(合格/不合格) 的主機。
- 報表檢視: 支援 WebAPI，可檢視其他管理中心的檢測報表。
- 合格統計: 提供整體合格數統計分析列表以及圖表，以及導入前、後合格數分析圖表。
- 資產管理: 統計整個單位軟體資產狀態，並提供軟體黑名單功能。
- 軟體派送: 可設定派送 .exe、.msi、msp 軟體至系統安裝/移除，包含軟體派送紀錄，軟體派送密碼保護。

管理中心功能

- 帳號管理: 支援密碼政策設定、帳戶鎖定。
- 登入管理: 可限制登入 IP 位址，支援一次性動態密碼(OTP) 登入驗證。
- 電腦列表: 可匯出 Excel 檔 (主機名稱、單位名稱、工作群組、IP 位址、作業系統、CPU、RAM、HardDisk)。
- 電腦列表: 可匯入 Excel 檔 (主機名稱、單位名稱、主機使用者、通知 email)，快速將主機分配至各個單位。