



WinMatrix IT 資源管理系統 3.8.31.x 版 週邊裝置安全管理模組功能規格表

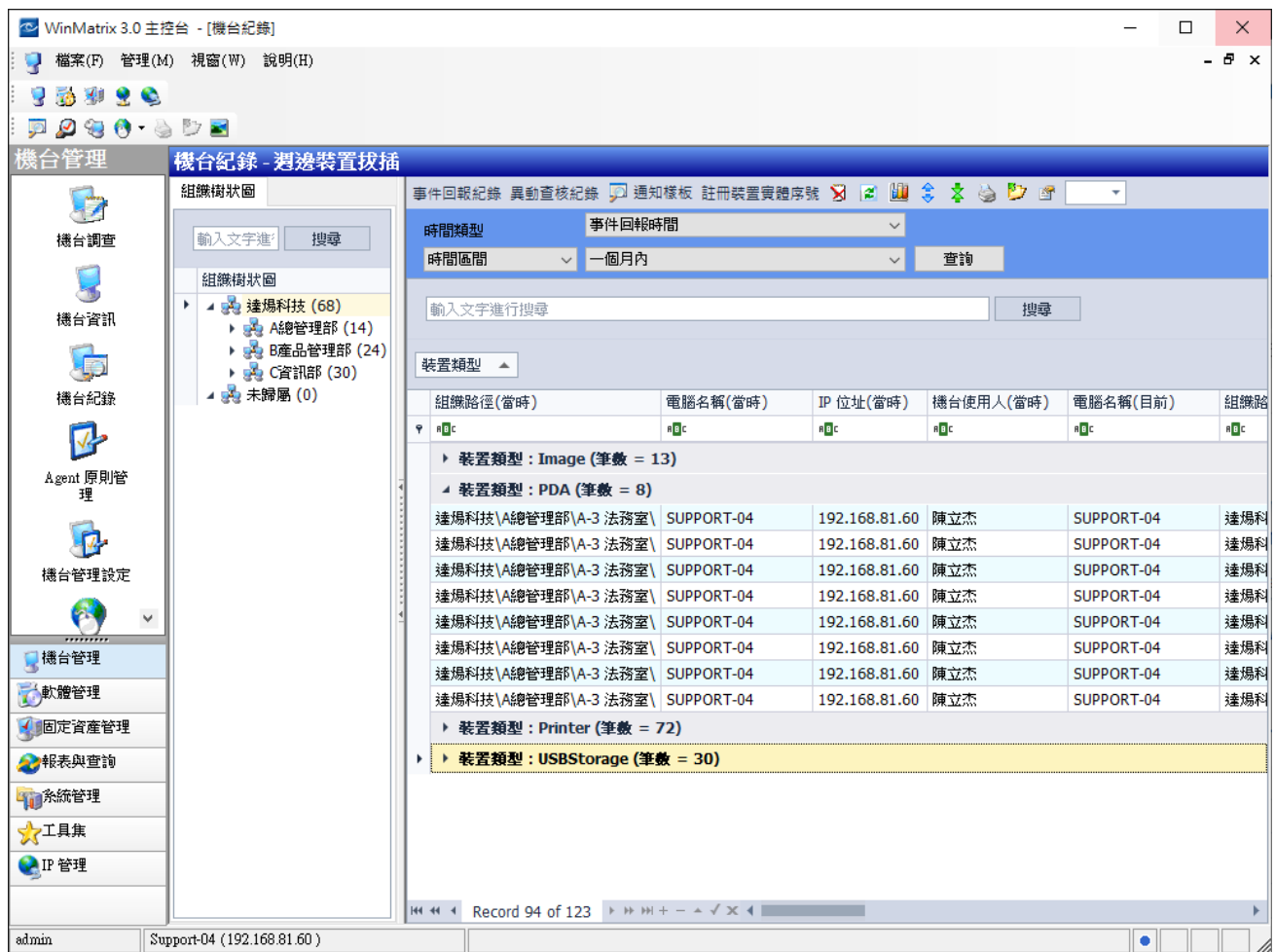
週邊裝置安全管理模組 (此為選購功能)		
電腦週邊裝置管制	功能效益	
	<ul style="list-style-type: none">禁止使用無線通訊（智慧型手機、4G、5G 無線上網、無線網卡、藍牙、紅外線），避免資料外洩，降低資訊安全風險。詳細記錄週邊裝置拔插行為，提供日後查詢與資安稽核。防範電腦具備多網路介面時，形成內外網同時並存的跳板機。	
	編號	功能項目
	1-1	簡易且彈性的管制原則套用模式： (1). 使用“Agent 原則”(policy)建立、套用的方式來規範電腦週邊裝置的使用權限(或使用模式)。 (2). “原則”(policy)套用的方式可依組織或電腦或 AD 登入帳號來設定。 (3). 可依星期、時間規範電腦週邊裝置是否可以使用，並支援多時段設定。 (4). 控管時段的設定種類提供：持續、指定時間、指定時段等方式，以滿足各種管控的情境。
	1-2	可將下列週邊裝置設定為 啟用/禁用/不管制： (1). 行動上網裝置/數據機 (2). 無線網路卡 (3). 實體網路卡 (4). 藍芽通訊裝置 (5). 紅外線通訊裝置 (6). IEEE1394 裝置 (7). PCMCIA 裝置 (8). USB 介面*1 (9). PDA 裝置/WPD 裝置 (10). LPT 埠裝置 (11). COM 埠裝置 (12). 智慧卡讀卡機 (13). 影像裝置 (14). 其他。依據 Windows 裝置管理員的裝置類型來設定。 當裝置的管制措施設為「不管制」時，WinMatrix 對於該裝置不會進行任何監控。通常是由其他系統控管該裝置，才會做「不管制」的設定。
	1-3	可禁止智慧型手機（如：iPhone、Andriod Phone）所模擬的網路卡。
1-4	週邊裝置若為隨插即用（PnP）的設備，其拔插使用時可被即時記錄。(自訂周邊裝置亦支援)	
1-5	可設定使用（插入/拔出）週邊裝置時，發出警示通知給使用者。管理者亦可設定接收訊息通報（Emai 或與畫面警示訊息視窗）。	

	1-6	可定期自動產生週邊裝置使用（插入/拔出）報表（日報表、週報表、月報表），協助資訊安全稽核。
進階電腦週邊裝置管制 - 自訂裝置管制條件	功能效益與應用情境	
	<ul style="list-style-type: none"> 使用裝置類別與裝置屬性作為管制條件，增加電腦週邊裝置的管制彈性。例如：公司內禁止使用光碟機，但由於市場上有些品牌的印表機在連接電腦時，會透過對應模擬出虛擬光碟機，提供對應的驅動程式安裝，因此 IT 管理人員可設定為除了印表機所模擬的光碟機外（依照裝置名稱），其餘光碟機一律禁用。讓管制機制可以同時兼顧組織內的使用現況與資訊安全的需求。 高管控完整性，可自行新增週邊裝置管制類型，涵蓋各式已知或未知的裝置：由於電腦週邊裝置種類繁多，因此 WinMatrix 提供設定上的彈性，新型裝置只須確認對應的 Windows 裝置類型後，就可以納入管制機制中。 	
	功能描述	
	2-1	<p>可依照裝置的屬性資料（裝置類型、裝置顯示名稱、列舉程式、製造廠商、裝置識別碼...等*2），管制電腦週邊裝置：</p> <p>(1). （正向表列管制）該類別裝置預設為全部禁用，只有符合特定屬性資料的裝置才可以使用。</p> <p>(2). （負向表列管制）該類別裝置預設為全部啟用，只有符合特定屬性資料的裝置才被禁用。</p>
	2-2	除 WinMatrix 已定義的裝置管制類型外，使用者可自行增加管制裝置的類型（Windows 作業系統所識別的裝置類別）。
網路稽核原則	功能效益與應用情境	
	<ul style="list-style-type: none"> 禁止電腦同時連通內部與外部網路，避免成為網路攻擊的跳板：管控筆記型電腦網路連線，禁止內部與外部網路同時連通。當筆記型電腦使用乙太網路連線至內部網路時，將自動關閉連線到外部無線分享器的無線網路卡，並顯示警示訊息。當使用者拔除了內部網路線（離開內部網路）後，系統將自動恢復無線網卡連線。自動化的機制同時兼顧了使用便利性與資訊安全。 防止電腦使用外部的網路，降低可能發生的資安風險。 依照可攜式電腦是否連接在組織內部網路，變更週邊裝置管制設定，增加管理彈性：管控筆記型電腦連線公司網路時，禁止使用 USB 隨身碟與燒錄光碟片，但當筆記型電腦帶回家中後，則可不受管制的正常使用。 	
	功能描述	
	3-1	<p>可設定當電腦離開內部網路、連通內部網路或連通外部網路時，WinMatrix 自動執行對應的矯正措施：</p> <p>(1). 顯示警示訊息或開啟指定網頁。</p> <p>(2). 自動執行特定命令。</p> <p>(3). 禁用/唯讀/開放指定的週邊裝置。（如：無線網卡、卸除式磁碟機）</p> <p>(4). 禁止非內部網路且連線中的實體網路卡。</p>

3-2	<p>可定義內部網路的判斷條件：</p> <ol style="list-style-type: none"> (1). 電腦 IP 設定：電腦所使用 IP 位址是否存在於內部網路所設定的 IP 範圍之中。 (2). 電腦連線 (Ping) 檢查：電腦是否可連線 (Ping) 到指定的伺服器。 (如：WinMatrix Server、AD) (3). 電腦連線 (TCP) 檢查：電腦是否可連線到指定的 TCP 通訊埠。
-----	--

2023.5.23.

<範例畫面>



The screenshot shows the WinMatrix 3.0 主控台 - [機台紀錄] window. The left sidebar contains a tree view with the following items: 機台調查, 機台資訊, 機台紀錄 (selected), Agent 原則管理, 機台管理設定, 機台管理, 軟體管理, 固定資產管理, 報表與查詢, 系統管理, 工具集, and IP 管理. The main area displays a table of device records. The table has columns: 組織路徑(當時), 電腦名稱(當時), IP 位址(當時), 機台使用人(當時), 電腦名稱(目前), and 組織路徑. The table is filtered by 裝置類型: Image (筆數 = 13) and 裝置類型: PDA (筆數 = 8). The table shows 13 records for Image devices and 8 records for PDA devices. The status bar at the bottom shows 'Record 94 of 123'.

組織路徑(當時)	電腦名稱(當時)	IP 位址(當時)	機台使用人(當時)	電腦名稱(目前)	組織路徑
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科
達揚科技\A總管理部\A-3 法務室\	SUPPORT-04	192.168.81.60	陳立杰	SUPPORT-04	達揚科



Agent 原則編輯

樣板名稱

22_原則-啟用網路稽核

☐ 預設值

描述

啟用網路稽核_未管制共用目錄

主要原則

週邊裝置原則

軟體原則

網站瀏覽管制

限制項目原則

網路稽核原則

安全模式原則

桌面管理

檔案目錄監控原則

高權限管理

本機群組管理

回報設定

硬體禁用

加密區設定

項目	類型	描述
軟碟機	標準	<預設權限為全部啟用>
光碟機	標準	<預設權限為全部啟用>
USB 卸除式磁碟	標準	日期：全部, 時間：全部, 工作日：全部, 權限：停用,
USB 介面	模組	<預設權限為全部啟用>
IEEE 1394 裝置	模組	<預設權限為全部啟用>
PCMCIA 裝置	模組	<預設權限為全部啟用>
COM Port 裝置	模組	<預設權限為全部啟用>
LPT Port 裝置	模組	<預設權限為全部啟用>
無線網路卡	模組	<預設權限為全部啟用>
實體網路卡	模組	<預設權限為不管制>
藍芽通訊裝置	模組	<預設權限為全部啟用>
紅外線裝置	模組	<預設權限為全部啟用>
PDA 裝置	模組	<預設權限為全部啟用>
智慧卡讀卡機	模組	<預設權限為全部啟用>
影像裝置	模組	<預設權限為全部啟用>
行動上網裝置 / 數據機	模組	<預設權限為全部啟用>

編輯

加入自訂管制裝置

移除自訂管制裝置

匯出

確定

取消



Agent 原則編輯

樣板名稱: 22_原則-啟用網路稽核 ☐ 預設值

描述: 啟用網路稽核_未管制共用目錄

主要原則 | 週邊裝置原則 | 軟體原則 | 網站瀏覽管制 | 限制項目原則 | 網路稽核原則 | 安全模式原則 | 桌面管理 | 檔案目錄監控原則 | 高權限管理 | 本機群組管理

☒ 啟用

內部網路條件

描述: 當符合下列設定值時, 機台視為存在於內部網路

加入 | 編輯 | 移除 | 複製

可連線 (Ping) 至	可連線 (TCP Port) 至	網路設定 IP 範圍位於
192.168.81.60;		192.168.81.1~192.168.81.254; 192.168.88.1~192.168.88.254;

稽核條件

當機台連通內部網路時 3

+ | - | X | Up | Down

類型	執行時機	描述
網路管制	符合稽核條件時執行	禁用非內部網路且連線中的實體網路卡: 是;
週邊裝置控制	符合稽核條件時執行	藍芽通訊裝置: 停用, 符合稽核條件時執行; PDA 裝置: 停用, 符合稽核條件時執行;

描述: 只能有一筆週邊裝置控制項目, 只能有一筆網路管制項目

匯出 | 確定 | 取消

*1 禁用 USB 介面時, 連接該介面的滑鼠、鍵盤、隨身碟...等裝置, 都將無法使用, 請小心設定。

標準功能模組即可針對隨身碟進行管控。

*2 依裝置類型的不同, 可設定的裝置管制屬性會有所差異。

* 若您需要更深入了解, 請洽電話: 02-2732-9516 或 Email: support@simopro.com 進行諮詢。